



Government Information Management System



Government Information Management System

OCIO Supports Section A

1. IM Advisory Services
 - 1.1. IM Advisory Services
 - 1.1.1. Capacity Development
 - 1.1.2. Education and Awareness
 - 1.1.3. Government Records Committee (GRC)
 - 1.1.4. Government Records Lifecycle Management (GRLM) & Provincial Records Centre
 - 1.2. Recent Projects
 - 1.3. HPRM (TRIM)

2. Training and Awareness Materials
 - 2.1. Training and Awareness
 - 2.2. GNL Orientation
 - 2.3. Information Management (IM) Month
 - 2.4. PS Access Courses

3. Capacity Supports
 - 3.1. IM Assessment Tools
 - 3.2. IM Capacity Building (IMCB) Tool Kit
 - 3.3. IM Policy Framework
 - 3.4. Public Bodies Listing (MOIA)

IM Legislative/Policy FrameworkSection B

- 1. Management of Information Act 1
- 2. Access to Information and Protection of Privacy Act 2
- 3. Policies 3
 - 3.1. Email Policy
 - 3.2. Information Management and Protection Policy
- 4. Directives 6
 - 4.1. Instant Messaging
 - 4.2. Acceptable Use of the Government Network and/or IT Assets
 - 4.3. Use of Non-Government Email Accounts for Work Purposes
- 5. Standards 10
 - 5.1. Developing One Time Disposal Submissions
 - 5.2. Developing Records Retention and Disposal Schedules for Operational Records
 - 5.3. Corporate Records Information Management Standard (C-RIMS)
- 6. Guidelines 14
 - 6.1. GNL Email Guidelines
 - 6.2. Discovery and Legal Hold
 - 6.3. Managing Departmental Information through the Employment Cycle
 - 6.4. Managing the Records of External Public Bodies
- 7. F.Y.I 19
 - 7.1. Acceptable Use of the GNL Network and/or Assets
 - 7.2. Which Records to Store in HPRM
 - 7.3. Secure Storage and Disposal of Physical Records
 - 7.4. Instant Messaging Directive
 - 7.5. Identifying and Disposing of Transitory Records
 - 7.6. Identification and Disposal of Government Records
 - 7.7. Records Retention and Disposal Schedule
 - 7.8. IM Advisory – Case Files
 - 7.9. IM Advisory – Executive Records
 - 7.10. IM Advisory – Meetings Records
 - 7.11. IM Advisory – Note to File
 - 7.12. IM Advisory – Program Administration Records

7.13. IM Advisory – Preparing Paper Records for Offsite Storage
 7.14. IM Advisory – Retrieving Records from the PRC
 7.15. IM Advisory – Transferring Records to the PRC

8. F.A.Q 20

8.1. Acceptable Use of the GNL Network and/or IT Assets
 8.2. Information Management and Protection Policy
 8.3. Instant Messaging
 8.4. Use of Non-Government Email Accounts for Work Purposes
 8.5. Corporate Records Information Management Standard (C-RIMS)
 8.6. Records Retention and Disposal Schedule
 8.7. One Time Disposal
 8.8. Government Records Committee
 8.9. Provincial Records Centre

9. Quick Reference 21

9.1. Transferring Records to The Rooms Provincial Archives Division
 9.2. Summary of ATIPP Exceptions
 9.3. Records Retention and Disposal Schedule Amendments
 9.4. Transitioning Instant Message Content to Recordkeeping Format

10. Templates 22

10.1. Records Retention and Disposal Schedule Template 1
 10.2. Records Retention and Disposal Schedule Template 2
 10.3. Memo – Request for Approval for RRDS for Submission to GRC
 10.4. Memo – Request for Approval for RRDS Amendment
 10.5. RRDS Amendment Summary of Changes
 10.6. Memo – Notification of Ownership Change
 10.7. One Time Disposal Submission Template
 10.8. Memo – Approval for One Time Disposal Submission
 10.9. Recordkeeping Guide

GRC RoleSection C

PRC Storage Section D

Guide to IM for Public BodiesSection E

- 1. Core IM Foundation 23
 - 1.1. IM Governance, Accountability and Organization
 - 1.2. IM Vision, Mission and Guiding Principles
 - 1.3. IM Legal and Regulatory Framework
 - 1.4. IM Program Plan

- 2. IM Program Components 28
 - 2.1. Information Management Policy Instruments
 - 2.2. Information Management Performance Measurement
 - 2.3. Education and Awareness for IM Practitioners
 - 2.4. IM Education and Awareness for Government Employees
 - 2.5. Physical Records Storage and Development and Use
 - 2.6. Information Protection

- 3. IM Tools 35
 - 3.1. Records and Information Inventory
 - 3.2. Classification Plan Development for Operational records
 - 3.3. Records Classification Plan Implementation
 - 3.4. Disposal of Records
 - 3.5. Record Imaging Services



Preface

The OCIO provides advisory services and support for government departments and supported public bodies to manage and protect information as part of their accountability under Section 6 of the Management of Information Act.

IM Services Division provides advisory services and support to government departments and other public bodies to build IM Capacity and enable compliance with legislation and IM best practices.

This binder is a compilation of all published materials and a description and update on all services provided by the IM Services division. It is designed as a ready reference of information on the various program components.



Section A

OCIO Supports

1. IM Advisory Services
 - 1.1. IM Advisory Services
 - 1.1.1. Capacity Development
 - 1.1.2. Education and Awareness
 - 1.1.3. Government Records Committee (GRC)
 - 1.1.4. Government Records Lifecycle Management (GRLM) & Provincial Records Centre
 - 1.2. Recent Projects
 - 1.3. HPRM (TRIM)
2. Training and Awareness Materials
 - 2.1. Training and Awareness
 - 2.2. GNL Orientation
 - 2.3. Information Management (IM) Month
 - 2.4. PS Access Courses
3. Capacity Supports
 - 3.1. IM Assessment Tools
 - 3.2. IM Capacity Building (IMCB) Tool Kit
 - 3.3. IM Policy Framework
 - 3.4. Public Bodies Listing (MOIA)



1. Advisory Services

Services offered by the Information Management Services Division (OCIO) are available to departments and other public bodies and can be grouped into the following categories:

- IM Advisory Services
- Capacity Development
- Education and Awareness
- Government Records Committee (GRC)
- Government Records Lifecycle Management (GRLM) & Provincial Records Centre

1.1. IM Advisory Services

- Provides general IM advice and guidance on existing IM policy instruments and the interpretation and application of IM legislation.
- Provides advice and consulting services to departments and supported entities in establishing and maintaining an IM program. Specific services include: guidance on records inventory requirements, records classification, records retention and disposal scheduling, recommendations on appropriate scanning processes and technology, guidance for data migration/conversions, and advice on IM policies, procedures and best practices.
- Provides front line HPRM/TRIM business functionality troubleshooting, including knowledge transfer and guidance. Facilitates TRIM Administrators Group meetings (TAG), conducts business process mapping sessions for classification in TRIM, and works closely with departmental TRIM Administrators to expand HPRM/TRIM business functionality.

1.1.1. Capacity Development

- The Information Management Self-Assessment Tool (IMSAT) program for public bodies is now complete. Public bodies should continue to self-assess their IM programs, benchmarking against previous scores, supporting capacity growth and risk reduction. IMSAT materials are available for re-use upon request.
- The IM Capacity Building (IMCB) Tool Kit is a support for public bodies to assist in building IM capacity within their organization. The Tool Kit is designed to support increased capacity and compliance through a continual improvement methodology, information asset management and the integration of tools, techniques and data analytics.

1.1.2. Education and Awareness

- Offers IM training in-class and online for GNL employees and IM professionals.
- Develops IM awareness materials for re-use by IM programs.
- Hosts IM Community meetings 3 times a year to provide an opportunity for information sharing among IM representatives at all levels across the broader public sector.

1.1.3. Government Records Committee

- The GRC is established by the Management of Information Act. The committee establishes and revises schedules for the retention, disposal, destruction or transfer of records; makes recommendations to the minister respecting government records to be forwarded to the archives; establishes disposal and destruction standards and guidelines for the lawful disposal and destruction of government records; and makes recommendations to the minister regarding the removal, disposal and destruction of records.
- Supports public bodies in submitting disposal and records retention schedule requests to the Government Records Committee (GRC), organizes GRC meetings, and communicates decisions made by the GRC to relevant public bodies.

1.1.4. Government Records Lifecycle Management & Provincial Records Centre (PRC)

- Provides guidance to public bodies on the appropriate disposal of government records.
- Operates the Provincial Records Centre (PRC), which provides a safe, secure storage facility for semi-active government records.
- PRC staff provide timely access to records in storage and facilitates the delivery and pick-up of records when needed.
- Provides administrative support to the Government Records Committee (GRC) and advice to public bodies on the process for submitting retentions schedules and one-time disposal requests for approval.
- Records storage is available to those public bodies whose information technology services are provided by the OCIO.

1.2. Recent Projects

Managing Your Email Activity Sessions

IM Advisory Services works with Departments providing coordination services, on site advice and individual employee guidance regarding their email inventory. The ability to assist employees in the determination of emails that can be considered government records and retained vs. those emails that may be transitory allows for employees to better manage process their Emails during such sessions.

These sessions promote the efficient management of electronic records through the creation, use, retention and disposal of government records ensuring that records disposed of during this process are authorized under the appropriate authority.

In January of this year (2019), the Department of Finance (under the support of departmental Executive) participated in a 3 day departmental wide initiative - where each branch were given the opportunity to participate.

HPRM Expansion – Department of Justice and Public Safety – High Sherriff’s Office

The High Sherriff of the Province identified a need to manage their Departmental records in an electronic format from creation onward and requested The Department of Justice and Public Safety to complete this work. A request submitted to the OCIO’s client services section and

resulted in IM Advisory Services Analysts providing a lead role in this project. Through IM Advisory Services HPRM expansion framework process, two IM Advisory Services analysts lead the client through the business/records analysis review, conducting a needs assessment and HPRM configuration. This work included developing, testing, implementation and training components, identification of the departmental records, management and use, including access and security of the records. As this request was determined to be small to medium scale work within an existing HPRM instance, it could be completed in-house by IM Advisory Services with no extra costing necessary.

Provincial Record Keeping Practices Standard Development – Department of CSSD – Adult Protection Division

The Adult Protection Division of the Department of Child Services and Seniors required a standard approach to current record keeping practices throughout their district offices. IM Advisory Services provided a lead role to this initiative. The work began in 2016 with a multiple phase approach within the four Health Authorities in the Province. Work included:

- Identifying current practices in each Health Authority and conducting a comparative analysis of inconsistencies in managing information throughout each Authority, categorizing gaps.
- Conduct stakeholder sessions to identify and review needs and inconsistencies
- Provided recommendations to the Steering Committee on gaps
- The end deliverable was the creation of 19 IM standards.

Corporate Records Management Standard – C-RIMS Update Initiative

C-RIMS is a standard classification plan designed to offer a nomenclature and classification rules for corporate records in all departments. It replaced the IMSAR standard released in 1999. Government has seen a dramatic increase in the ways and means of creating, managing, storing and disposing of records in a hybrid environment in which both paper and electronic records are used, C-RIMS can be used to assist in the management of these paper and/or electronic records throughout the lifecycle.

The changing Government landscape and organization structure and consistent advancements in technology has necessitated the need to review this current standard and provide updated guidance on the management and disposition of corporate records. IM Advisory Services is leading this work with the first update set to be released in June, 2019 of the Financial section of the Standard.

1.3. HPRM (formerly TRIM)

HP Records Manager (formerly TRIM) is the Government of Newfoundland and Labrador standard solution for electronic document and records management. At present, there are 54 TRIM instances in use throughout core Government Departments and 2 more under development. This is an enterprise wide solution that enables Departments to move forward with such initiatives as electronic case file management, Correspondence Management and business process automation.

IM Advisory Services supports TRIM Program initiatives, expansion activities and functionality through the application of dedicated staff that support TRIM Administrators in these areas.
HPRM (TRIM) Administrators Support:

- The TRIM Administrators Group (TAG) is a community of practice dedicated to TRIM Administrators that promotes information sharing and education on various functions and configuration schemes in a business process in TRIM. This group meets quarterly for subject matter presentations, to discuss common topics; FYI's and collaborates on areas of mutual interest. The goal is to allow TRIM Administrators an opportunity to work collectively to analyze and resolve issues, to share successes and lessons learned, develop best practices and to promote the expansion and use of HPRM.
- IM Advisory Services will work with TRIM Administrators to expand the use of HPRM in their department.
- Also offered is routine troubleshooting of functional issues within a particular HPRM instance.

HPRM (TRIM) Program Support:

- Works with other areas in OCIO to identify and process HPRM-related client issues.
- Provides expertise regarding a client's business needs, and HPRM functionality to OCIO project teams.
- Advises and sits on the TRIM Program Committee.
- Manages TRIM client training needs requests.



2. Training and Awareness Materials

2.1. Training and Awareness

Education and Awareness is an essential component of an Information Management (IM) Program. Public Service employees are required to have a clear understanding of their IM responsibilities, and how they can support IM compliance in their department or public body. Ongoing awareness and training by OCIO contribute to building IM capacity growth across government. This continued training is especially essential in order to stay ahead of emerging technologies and meet the demands of our clients and their business functions.

The OCIO has a comprehensive education and awareness program to support employee compliance with IM requirements and best practices.

IM Materials Developed Summary for Fiscal 2018-2019

- IM Month Campaign
- IM Advisories
- IM Tips
- Email Guideline Update
- Managing Transitory Records
- Multi Mailbox Processing

- Employee Life Cycle Guideline - Update
- IM Guide for Public Bodies
- IM Website Updates
- Use of Non-Government Email Accounts for Work Purposes Directive – Update
- Supporting IM@OCIO with Forms Management
- Supporting Cabinet Secretariat/Legal Team with Disclosure for Muskrat Falls Inquiry

IM Training and Awareness Conducted for Fiscal 2018-2019

- IM Community Sessions 3 Sessions
- Auditor General (AG) Disclosure Overview/Training1 Session
- IM Program Plan 2 Sessions
- Introduction to IM Processes.....1 Session
- Multi-Mailbox Session 3 Sessions
- Managing Transitory Records 12 Sessions

IM Community meetings are conducted quarterly typically in Jan, April and Sept. The IM community is the OCIO’s largest community of practice. Membership is open to anyone working in the public sector that whose position involves direct IM work. Information sessions are conducted on evolving IM issues and internal and external expertise is sought to provide advice on IM best practices.

2.2. GNL Orientation

A Director/Manager is responsible for ensuring that each new employee receives a comprehensive onboarding experience. This involves reviewing the government wide “Onboarding Checklist” located at:

https://www.exec.gov.nl.ca/exec/hrs/learning_and_development/onboarding.html

This checklist involves IM policies and online training that employees can take advantage of to ensure they are aware of their IM responsibilities.

IM policies and online training include:

- Office of the Chief Information Officer (OCIO) Policies and Guidelines:
www.ocio.gov.nl.ca/ocio/policies/index.html
- Access to Information and Protection of Privacy (ATIPP) e-learning:
<https://login.psaccess.ca/>
- Management of Information Act (MOIA):
<https://assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>
- Information Management (IM@Work) e-learning
<https://login.psaccess.ca/>
- Information Management (IM@Work) presentation
www.ocio.gov.nl.ca/ocio/im/practitioners/pdf
- Information Management: A Guide for Managers
<https://login.psaccess.ca/>
- Cyber Security Awareness e-learning:
<https://login.psaccess.ca/>

2.3. Information Management (IM) Month

Information Management (IM) Month is celebrated internationally during the month of April to promote both the IM profession and to highlight the impact that IM has on business activities. The purpose is to emphasize the value and importance of organizing and maintaining records in all media for the efficient and effective management of any organization.

Recognizing that all public servants have a valuable role to play in managing information and in creating records, this year (2019), the OCIO's IM Month campaign theme was "For the Record, That's a Record". The Office of the Chief Information Officer (OCIO) supports employees with IM learning resources and best practices in order to promote an IM-conscious work environment.

Government records can come in many formats such as instant messages, paper, maps, drawings, email, paintings, photographs, magnetic tapes, computer discs, microform and other documentary material regardless of physical form or characteristic.

Government records should be an accurate and complete reflection of the business affairs conducted. In creating or retaining government records, it is important for departments and public bodies to ensure the quality of information contained is sufficient, as they may have to be provided in the event of a legal, audit, inquiry, or review disclosure processes (e.g. ATIPPA).

For the 2019 IM Month campaign the OCIO encouraged public servants to practice good IM, some tips include:

- CREATE – Understand the records you are responsible to create and properly manage – discuss with your supervisor;
- TRANSFER – Deal with your Emails or other e-records as it arrives by either cataloguing it appropriately (i.e. HPRM, shared drive) or dispose of it if transitory;
- CLEAN-UP - Use the “Conversation Clean- Up” tool to assist in managing email.

2.4. PS Access Courses

The following is a listing of IM/IP PS Access Courses:

- Information Management (IM@Work) e-learning
<https://login.psaccess.ca/>
- Information Management: A Guide for Managers
<https://login.psaccess.ca/>
- Cyber Security Awareness e-learning:
<https://login.psaccess.ca/>



3. Capacity Supports

3.1. IM Assessment Tools

- IM Capacity Assessment Tool (IMCAT) was delivered from 2007 to 2013 (35 Assessments).
- IM Self-Assessment Tool (IMSAT) was delivered from 2015 to 2018 (25 Assessments). Public bodies should continue to self-assess their IM programs, benchmarking against previous scores, supporting capacity growth and risk reduction. IMSAT materials are available for re-use upon request.
- IM Check-Up is underway as of February 2019. The new program leverages past assessments as well as current materials to support public body directors with responsibility for IM and their staff in moving forward in legislative compliance and growing IM capacity.

3.2. IM Capacity Building (IMCB) Tool Kit

- IMCB Tool Kit is a support for public bodies to assist in building IM capacity within their organization serving to reduce IM risk and increase public body compliance with the Management of Information Act (MOIA).
- IMCB Tool Kit is designed to support increased capacity and compliance through a continual improvement methodology, information asset management and the integration of tools, techniques and data analytics.

3.3. IM Policy Framework

- Establish an inventory of all materials, governance, audience and topics.
- Standardization through the development and use of IM Services templates, processes and style guide.

3.4. Public Bodies Listing (MOIA)

- Currently there are 163 public bodies (updated December 2018) as defined by the 5 part definition for public bodies under MOIA.
- Assessments such as the IMSAT and IM Check-Up review the listing with the reporting entities (departments) and leverage the reporting entities to communicate with and share the requirements as outlined with the MOIA and the IM&P Policy



Section B

IM Legislative/Policy Framework

1. Management of Information Act.....	1
2. Access to Information and Protection of Privacy Act	2
3. Policies	3
3.1. Email Policy	
3.2. Information Management and Protection Policy	
4. Directives	6
4.1. Instant Messaging	
4.2. Acceptable Use of the Government Network and/or IT Assets	
4.3. Use of Non-Government Email Accounts for Work Purposes	
5. Standards	10
5.1. Developing One Time Disposal Submissions	
5.2. Developing RRDS for Operational Records	
5.3. Corporate Records Information Management Standard (C-RIMS)	
6. Guidelines	14
6.1. GNL Email Guidelines	
6.2. Discovery and Legal Hold	
6.3. Managing Departmental Information through the Employment Cycle	
6.4. Managing the Records of External Public Bodies	

7. F.Y.I	19
7.1. Acceptable Use of the GNL Network and/or Assets	
7.2. Which Records to Store in HPRM	
7.3. Secure Storage and Disposal of Physical Records	
7.4. Instant Messaging Directive	
7.5. Identifying and Disposing of Transitory Records	
7.6. Identification and Disposal of Government Records	
7.7. Records Retention and Disposal Schedule	
7.8. IM Advisory – Case Files	
7.9. IM Advisory – Executive Records	
7.10. IM Advisory – Meetings Records	
7.11. IM Advisory – Note to File	
7.12. IM Advisory – Program Administration Records	
7.13. IM Advisory – Preparing Paper records for Offsite Storage	
7.14. IM Advisory – Retrieving Records from the PRC	
7.15. IM Advisory – Transferring Records to the PRC	
8. F.A.Q	20
8.1. Acceptable Use of the GNL Network and/or IT Assets	
8.2. Information Management and Protection Policy	
8.3. Instant Messaging	
8.4. Use of Non-Government Email Accounts for Work Purposes	
8.5. Corporate Records Information Management Standard (C-RIMS)	
8.6. Records Retention and Disposal Schedule	
8.7. One Time Disposal	
8.8. Government Records Committee	
8.9. Provincial Records Centre	
9. Quick Reference	21
9.1. Transferring Records to The Rooms Provincial Archives Division	
9.2. Summary of ATIPP Exceptions	
9.3. Records Retention and Disposal Schedule Amendments	
9.4. Transitioning Instant Message Content to Recordkeeping Format	
10. Templates	22
10.1. Records Retention and Disposal Schedule Template 1	
10.2. Records Retention and Disposal Schedule Template 2	
10.3. Memo – Request for Approval for RRDS for Submission to GRC	
10.4. Memo – Request for Approval for RRDS Amendment	
10.5. RRDS Amendment Summary of Changes	
10.6. Memo – Notification of Ownership Change	

- 10.7. One Time Disposal Submission Template
- 10.8. Memo – Approval for One Time Disposal Submission
- 10.9. Recordkeeping Guide



1. Management of Information Act

This is an official version.

Copyright © 2017: Queens Printer,
St. John's, Newfoundland and Labrador, Canada

Important Information

(Includes details about the availability of printed and electronic versions of the Statutes.)

[Table of Public Statutes](#)

[Main Site](#)

[How current is this statute?](#)

[Responsible Department](#)

SNL2005 CHAPTER M-1.01

MANAGEMENT OF INFORMATION ACT

Amended:

2008 c54; [2016 cR-15.2 s33](#) (not in force-not included)

CHAPTER M-1.01

AN ACT RESPECTING THE MANAGEMENT OF GOVERNMENT INFORMATION FOR THE PROVINCE

(Assented to May 19, 2005)

Analysis

- [1. Short title](#)
- [2. Definitions](#)
- [3. Application](#)
- [4. Crown property](#)
 - [4.1 Electronic information](#)
- [5. Management of government records](#)
 - [5.1 Government Records Committee](#)
 - [5.2 Removal and destruction of records](#)
 - [5.3 Dispute](#)
 - [5.4 Exceptions](#)
- [6. System for management of information](#)
 - [7. Application](#)
 - [7.1 Regulations](#)

[8. Offence](#)[9. RSNL1990 cA-16 Rep.](#)

Be it enacted by the Lieutenant-Governor and House of Assembly in Legislative Session convened, as follows:

Short title

1. This Act may be cited as the *Management of Information Act* .

[2005 cM-1.01 s1](#)

[Back to Top](#)**Definitions**

2. In this Act

- (a) "abandoned record" means a government record to which ownership cannot be established and which has been determined to be an abandoned record by the chief information officer;
- (a.1) "archives" means The Rooms Provincial Archives referred to in section 21 of the *Rooms Act* ;
- (a.2) "cabinet record" means a record that
 - (i) is a memorandum, the purpose of which is to present proposals or recommendations to Cabinet,
 - (ii) is a discussion paper, policy analysis, proposal, advice or briefing material, including all factual and background material prepared for Cabinet,
 - (iii) is an agenda, minute or other record of Cabinet recording deliberations or decisions of Cabinet,
 - (iv) is used for or reflects communications or discussions among ministers on matters relating to the making of government decisions or the formulation of government policy,
 - (v) is created for or by a minister for the purpose of briefing that minister on a matter for Cabinet,
 - (vi) is created during the process of developing or preparing a submission for Cabinet,
 - (vii) is draft legislation or a draft regulation, or
 - (viii) contains information about the contents of a record within a class of information referred to in subparagraphs (i) to (vii);
- (a.3) "chief information officer" means the Chief Information Officer of the Office of the Chief Information Officer;
- (a.4) "committee" means the committee established under section 5.1;
- (b) "department", unless the context indicates otherwise, means the department presided over by the minister;

- (b.1) "government record" means a record created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and an abandoned record;
- (c) "minister", unless the context indicates otherwise, means the minister appointed under the *Executive Council Act* to be responsible for this Act;
- (d) "public body" means
- (i) a department created under the *Executive Council Act* or a branch of the executive government of the province,
 - (ii) a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown,
 - (iii) a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a minister of the Crown,
 - (iv) a court established under an Act of the province, and
 - (v) the House of Assembly and committees of the House of Assembly;
- (e) [Rep. by 2008 c54 s2]
- (f) "record" means a correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic;
- (g) "record management" means a program of record and information management instituted to provide an economical and efficient system for the creation, maintenance, retrieval and disposal of government records; and
- (h) "transitory record" means a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

[2005 cM-1.01 s2; 2008 c54 ss1&2](#)

[Back to Top](#)

Application

3. This Act applies to all public bodies in the province.

[2005 cM-1.01 s3](#)

[Back to Top](#)

Crown property

4. (1) All records created by or received by a public body in the conduct of its affairs are the property of the Crown.

- (2) Records referred to in subsection (1) shall not be destroyed or removed from the ownership or control of the Crown unless the destruction or removal is authorized under this Act.

[2008 c54 s3](#)

[Back to Top](#)

Electronic information

4.1 (1) A requirement under this Act to retain a record is satisfied by the retention of electronic information where

- (a) the electronic information is retained in the format in which it was made, sent or received or in a format that does not materially change the electronic information that was originally created, sent or received; and
- (b) the electronic information will be accessible, and capable of being retained for subsequent reference, if required, by a person who is entitled to have access to the information or who is authorized to require its production.

(2) Where the electronic information was sent or received, the requirement in subsection (1) is only met where information that identifies the origin and destination of the electronic information and the date and time when it was sent or received is also retained.

(3) Nothing in this section prevents the disposal of electronic records according to a process or schedule approved under this Act.

[2008 c54 s4](#)

[Back to Top](#)

Management of government records

5. (1) The minister shall

- (a) be responsible for the development and implementation of a management program for government records in the province;
- (b) provide advice to and assist public bodies with the development, implementation and maintenance of record management systems and provide direction on that material as it relates to the preservation of potential archival material; and
- (c) recommend standards, principles or procedures to the Treasury Board for adoption.

(2) The minister may, in the manner permissible by law, appoint and employ those persons necessary to carry out the purposes of this Act.

(3) A person appointed or employed under subsection (2) to be responsible for information and record management shall consult with the Director of The Rooms Provincial Archives appointed under section 22 of the *Rooms Act* to ensure the efficient implementation of information management policies and procedures for the preservation of archival government records.

[2005 cM-1.01 s5; 2008 c54 ss1&5](#)

[Back to Top](#)

Government Records Committee

5.1 (1) There shall be a committee to be known as the Government Records Committee consisting of

- (a) the Director of The Rooms Provincial Archives appointed under section 22 of the *Rooms Act* ;
- (b) the Deputy Minister of Justice or a person designated by him or her to act on his or her behalf;
- (c) the Deputy Minister of Finance or a person designated by him or her to act on his or her behalf;
- (d) the Chief Information Officer or a person designated by him or her to act on his or her behalf; and
- (e) those other persons whom the minister may appoint.

(2) The person appointed under subsection (1)(d) or a person designated by him or her to act on his or her behalf shall be the chairperson of the committee.

(3) The committee shall designate from among its members a person who shall be the secretary for the committee.

(4) The Office of the Chief Information Officer shall provide administrative support for the committee in order to assist the committee in executing its powers and duties.

(5) The committee may

- (a) establish and revise schedules for the retention, disposal, destruction or transfer of records;
- (b) make recommendations to the minister respecting government records to be forwarded to the archives;
- (c) establish disposal and destruction standards and guidelines for the lawful disposal and destruction of government records; and
- (d) make recommendations to the minister regarding the removal, disposal and destruction of records.

(6) A decision of a majority of the members of the committee shall be the decision of the committee.

[2008 c54 s6](#)

[Back to Top](#)

Removal and destruction of records

5.2 The minister may, after considering recommendations of the committee under subsection 5.1 (5), direct the removal, disposal or destruction of records.

[2008 c54 s6](#)

[Back to Top](#)

Dispute

5.3 Where a dispute arises between a public body and the committee with respect to the

- (a) adoption or operation of a disposal schedule; or

- (b) destruction or disposal of government records,

the committee may submit the matter to the minister who may issue directions with respect to the dispute.

[2008 c54 s6](#)

[Back to Top](#)

Exceptions

5.4 (1) Cabinet records shall be managed in the manner determined by Cabinet Secretariat.

(2) The chief information officer may determine that records are abandoned records and shall transfer the custody of those records to the Director of The Rooms Provincial Archives appointed under section 22 of the *Rooms Act* who shall dispose of the records in accordance with this Act.

(3) Transitory records may be disposed of when they are no longer of value, and shall only be disposed of through means which render them unreadable, including secure shredding or in the case of electronic records, secure electronic erasure.

(4) Records that may present a health or biohazard may be disposed of in a manner determined by the committee.

[2008 c54 s6](#)

[Back to Top](#)

System for management of information

6. (1) A permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records.

(2) A system required under subsection (1) shall provide for retention periods and disposition by

- (a) destruction, or
- (b) transfer to the archives,

in accordance with the guidelines and schedules established by the Government Records Committee established under section 5.1.

(3) A permanent head of a public body shall ensure that the retention, disposal and removal of government records is carried out in accordance with this Act.

[2005 cM-1.01 s6; 2008 c54 ss1&7](#)

[Back to Top](#)

Application

7. The minister may apply for an order under rule 27 of the *Rules of the Supreme Court, 1986* for the recovery of government records to which a public body is entitled.

[2005 cM-1.01 s7; 2008 c54 s1](#)

[Back to Top](#)

Regulations

7.1 The Lieutenant-Governor in Council may make regulations

- (a) respecting the procedures and duties of the committee established under section 5.1; and
- (b) generally to give effect to the purpose of this Act.

[2008 c54 s8](#)

[Back to Top](#)

Offence

8. (1) A person who unlawfully damages, mutilates or destroys a government record or removes or withholds a government record from the possession of a public body or otherwise violates this Act is guilty of an offence and is liable on summary conviction to a fine of not less than \$1,000 and not more than \$50,000 and in default of payment to imprisonment for a term of not less than 3 months and not more than 18 months or to both a fine and imprisonment.

(2) In addition to a penalty imposed under subsection (1) a judge may make an order that the record that is the subject of an offence be returned to the possession of the public body.

[2005 cM-1.01 s8](#); [2008 c54 s1](#)

[Back to Top](#)

RSNL1990 cA-16 Rep.

9. *The Archives Act* is repealed.

[2005 cM-1.01 s9](#)

©Queen's Printer



2. Access to Information and Protection of Privacy Act

This is an official version.

Copyright © 2019: Queen's Printer,
St. John's, Newfoundland and Labrador, Canada

Important Information

(Includes details about the availability of printed and electronic versions of the Statutes.)

[Table of Public Statutes](#)

[Main Site](#)

[How current is this statute?](#)

[Responsible Department](#)

SNL2015 CHAPTER A-1.2

**ACCESS TO INFORMATION AND PROTECTION
OF PRIVACY ACT, 2015**

Amended:

2016 c6 s2; 2016 cR-15.2 s30 (not in force-not included); 2017 c10 s3; 10/18 s2; 2018 c1 s1; 2018
cI-7.1 s24
2018 cC-12.3 s112

CHAPTER A-1.2

**AN ACT TO PROVIDE THE PUBLIC WITH ACCESS TO INFORMATION
AND PROTECTION OF PRIVACY**

(Assented to June 1, 2015)

Analysis

[1. Short title](#)

PART I
INTERPRETATION

[2. Definitions](#)

[3. Purpose](#)

[4.
Schedule of excluded public bodies](#)

[5. Application](#)

[6. Relationship to Personal Health Information Act](#)

[7. Conflict with other Acts](#)

PART II
ACCESS AND CORRECTION

DIVISION 1
THE REQUEST

- [8. Right of access](#)
- [9. Public interest](#)
- [10. Right to request correction of personal information](#)
- [11. Making a request](#)
- [12. Anonymity](#)
- [13. Duty to assist applicant](#)
- [14. Transferring a request](#)
- [15. Advisory response](#)
- [16. Time limit for final response](#)
- [17. Content of final response for access](#)
- [18. Content of final response for correction of personal information](#)
- [19. Third party notification](#)
- [20. Provision of information](#)
- [21. Disregarding a request](#)
- [22. Published material](#)
- [23. Extension of time limit](#)
- [24. Extraordinary circumstances](#)
- [25. Costs](#)
- [26. Estimate and waiver of costs](#)

DIVISION 2
EXCEPTIONS TO ACCESS

- [27. Cabinet confidences](#)
- [28. Local public body confidences](#)
- [29. Policy advice or recommendations](#)
- [30. Legal advice](#)
- [31. Disclosure harmful to law enforcement](#)
- [32. Confidential evaluations](#)
- [33. Information from a workplace investigation](#)
- [34. Disclosure harmful to intergovernmental relations or negotiations](#)
- [35. Disclosure harmful to the financial or economic interests of a public body](#)
- [36. Disclosure harmful to conservation](#)
- [37. Disclosure harmful to individual or public safety](#)
- [38. Disclosure harmful to labour relations interests of public body as employer](#)
- [39. Disclosure harmful to business interests of a third party](#)
- [40. Disclosure harmful to personal privacy](#)
- [41. Disclosure of House of Assembly service and statutory office records](#)

DIVISION 3
COMPLAINT

- [42. Access or correction complaint](#)
- [43. Burden of proof](#)
- [44. Investigation](#)
- [45. Authority of commissioner not to investigate a complaint](#)
- [46. Time limit for formal investigation](#)
- [47. Recommendations](#)
- [48. Report](#)
- [49. Response of public body](#)
- [50. Head of public body seeks declaration in court](#)
- [51. Filing an order with the Trial Division](#)

DIVISION 4
APPEAL TO THE TRIAL DIVISION

- [52. Direct appeal to Trial Division by an applicant](#)
- [53. Direct appeal to Trial Division by a third party](#)
- [54. Appeal of public body decision after receipt of commissioner's recommendation](#)
- [55. No right of appeal](#)
- [56. Procedure on appeal](#)
- [57. Practice and procedure](#)
- [58. Solicitor and client privilege](#)
- [59. Conduct of appeal](#)
- [60. Disposition of appeal](#)

PART III
PROTECTION OF PERSONAL INFORMATION

DIVISION 1
COLLECTION, USE AND DISCLOSURE

- [61. Purpose for which personal information may be collected](#)
- [62. How personal information is to be collected](#)
- [63. Accuracy of personal information](#)
- [64. Protection of personal information](#)
- [65. Retention of personal information](#)
- [66. Use of personal information](#)
- [67. Use of personal information by post-secondary educational bodies](#)
- [68. Disclosure of personal information](#)
- [69. Definition of consistent purposes](#)
- [70. Disclosure for research or statistical purposes](#)
- [71. Disclosure for archival or historical purposes](#)
- [72. Privacy impact assessment](#)

DIVISION 2
PRIVACY COMPLAINT

- [73. Privacy complaint](#)

- [74. Investigation – privacy complaint](#)
- [75. Authority of commissioner not to investigate a privacy complaint](#)
- [76. Recommendations – privacy complaint](#)
- [77. Report – privacy complaint](#)
- [78. Response of public body – privacy complaint](#)
- [79. Head of public body seeks declaration in court](#)
- [80. Filing an order with the Trial Division](#)

DIVISION 3
APPLICATION TO THE TRIAL DIVISION FOR A DECLARATION

- [81. Practice and procedure](#)
- [82. Solicitor and client privilege](#)
- [83. Conduct](#)
- [84. Disposition](#)

PART IV
OFFICE AND POWERS OF THE INFORMATION AND PRIVACY COMMISSIONER

DIVISION 1
OFFICE

- [85. Appointment of the Information and Privacy Commissioner](#)
- [86. Status of the commissioner](#)
- [87. Term of office](#)
- [88. Removal or suspension](#)
- [89. Acting commissioner](#)
- [90. Salary, pension and benefits](#)
- [91. Expenses](#)
- [92. Commissioner's staff](#)
- [93. Oath of office](#)
- [94. Oath of staff](#)

DIVISION 2
POWERS OF THE COMMISSIONER

- [95. General powers and duties of commissioner](#)
- [96. Representation during an investigation](#)
- [97. Production of documents](#)
- [98. Right of entry](#)
- [99. Admissibility of evidence](#)
- [100. Privilege](#)
- [101. Section 8.1 of the Evidence Act](#)
- [102. Disclosure of information](#)
- [103. Delegation](#)
- [104. Protection from liability](#)
- [105. Annual report](#)

- [106. Special report](#)
- [107. Report – investigation or audit](#)
- PART V
GENERAL
- [108. Exercising rights of another person](#)
- [109. Designation of head by local public body](#)
- [110. Designation and delegation by the head of a public body](#)
- [111. Publication scheme](#)
- [112. Amendments to statutes and regulations](#)
- [113. Report of minister responsible](#)
- [114. Limitation of liability](#)
- [115. Offence](#)
- [116. Regulations](#)
- [117. Review](#)
- [118. Transitional](#)
- [119. SNL2013 cA-3.1 Amdt.](#)
- [120. SNL1991 c22 Amdt.](#)
- [121. RSNL1990 cC-2 Amdt.](#)
- [122. SNL2004 cC-5.1 Amdt.](#)
- [123. SNL2010 cC-12.2 Amdt.](#)
- [124. SNL2001 cC-14.1 Amdt.](#)
- [125. SNL2007 cE-11.01 Amdt.](#)
- [126. SNL1995 cP-37.1 Amdt.](#)
- [127. RSNL1990 cH-10 Amdt.](#)
- [128. SNL2007cH-10.1 Amdt.](#)
- [129. SNL1999 cM-5.1 Amdt.](#)
- [130. SNL2014 cM-16.2 Amdt.](#)
- [131. SNL2008 cP-7.01 Amdt.](#)
- [132. SNL2008 cR-13.1 Amdt.](#)
- [133. SNL2014 c23 Amdt.](#)
- [134. SNL2005 cR-15.1 Amdt.](#)
- [135. SNL2009 cV-6.01 Amdt.](#)
- [136. Repeal](#)
- [137. Commencement](#)

- [Schedule A](#)

- [Schedule B](#)

Be it enacted by the Lieutenant-Governor and House of Assembly in Legislative Session convened, as follows:

Short title

1. This Act may be cited as the *Access to Information and Protection of Privacy Act, 2015* .

[2015 cA-1.2 s1](#)

**PART I
INTERPRETATION**

[Back to Top](#)

Definitions

2. In this Act

- (a) "applicant" means a person who makes a request under section 11 for access to a record, including a record containing personal information about the person, or for correction of personal information;
- (b) "business day" means a day that is not a Saturday, Sunday or a holiday;
- (c) "Cabinet" means the executive council appointed under the *Executive Council Act* , and includes a committee of the executive council;
- (d) "commissioner" means the Information and Privacy Commissioner appointed under section 85 ;
- (e) "complaint" means a complaint filed under section 42 ;
- (f) "coordinator" means the person designated by the head of the public body as coordinator under subsection 110 (1);
- (g) "dataset" means information comprising a collection of information held in electronic form where all or most of the information in the collection
- (i) has been obtained or recorded for the purpose of providing a public body with information in connection with the provision of a service by the public body or the carrying out of another function of the public body,
- (ii) is factual information
- (A) which is not the product of analysis or interpretation other than calculation, and
- (B) to which section 13 of the *Statistics Agency Act* does not apply, and
- (iii) remains presented in a way that, except for the purpose of forming part of the collection, has not been organized, adapted or otherwise materially altered since it was obtained or recorded;
- (h) "educational body" means
- (i) Memorial University of Newfoundland ,
- (ii) College of the North Atlantic ,
- (iii) Centre for Nursing Studies,

- (iv) Western Regional School of Nursing,
- (v) a school board, school district constituted or established under the *Schools Act, 1997*, including the conseil scolaire francophone, and
- (vi) a body designated as an educational body in the regulations made under section 116 ;
- (i) "employee", in relation to a public body, includes a person retained under a contract to perform services for the public body;
- (j) "head", in relation to a public body, means
 - (i) in the case of a department, the minister who presides over it,
 - (ii) in the case of a corporation, its chief executive officer,
 - (iii) in the case of an unincorporated body, the minister appointed under the *Executive Council Act* to administer the Act under which the body is established, or the minister who is otherwise responsible for the body,
 - (iv) in the case of the House of Assembly the Speaker and in the case of the statutory offices as defined in the *House of Assembly Accountability, Integrity and Administration Act*, the applicable officer of each statutory office, or
 - (v) in another case, the person or group of persons designated under section 109 or in the regulations as the head of the public body;
- (k) "health care body" means
 - (i) an authority as defined in the *Regional Health Authorities Act* ,
 - (ii) the Mental Health Care and Treatment Review Board,
 - (iii) the Newfoundland and Labrador Centre for Health Information, and
 - (iv) a body designated as a health care body in the regulations made under section 116 ;
- (l) "House of Assembly Management Commission" means the commission continued under section 18 of the *House of Assembly Accountability, Integrity and Administration Act* ;
- (m) "judicial administration record" means a record containing information relating to a judge, master or justice of the peace, including information respecting
 - (i) the scheduling of judges, hearings and trials,
 - (ii) the content of judicial training programs,
 - (iii) statistics of judicial activity prepared by or for a judge,
 - (iv) a judicial directive, and
 - (v) a record of the Complaints Review Committee or an adjudication tribunal established under the *Provincial Court Act, 1991* ;
- (n) "law enforcement" means

- (i) policing, including criminal intelligence operations, or
 - (ii) investigations, inspections or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead to or could lead to a penalty or sanction being imposed under the enactment;
- (o) "local government body" means
- (i) the City of Corner Brook ,
 - (ii) the City of Mount Pearl ,
 - (iii) the City of St. John's ,
 - (iv) a municipality as defined in the *Municipalities Act, 1999* , and
 - (v) a body designated as a local government body in the regulations made under section 116 ;
- (p) "local public body" means
- (i) an educational body,
 - (ii) a health care body, and
 - (iii) a local government body;
- (q) "minister" means a member of the executive council appointed under the *Executive Council Act* ;
- (r) "minister responsible for this Act" means the minister appointed under the *Executive Council Act* to administer this Act;
- (s) "officer of the House of Assembly" means the Speaker of the House of Assembly, the Clerk of the House of Assembly, the Chief Electoral Officer, the Auditor General of Newfoundland and Labrador, the Commissioner for Legislative Standards, the Citizens' Representative, the Child and Youth Advocate, the Seniors' Advocate and the Information and Privacy Commissioner, and a position designated to be an officer of the House of Assembly by the Act creating the position;
- (t) "person" includes an individual, corporation, partnership, association, organization or other entity;
- (u) "personal information" means recorded information about an identifiable individual, including
- (i) the individual's name, address or telephone number,
 - (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
 - (iii) the individual's age, sex, sexual orientation, marital status or family status,
 - (iv) an identifying number, symbol or other particular assigned to the individual,
 - (v) the individual's fingerprints, blood type or inheritable characteristics,

- (vi) information about the individual's health care status or history, including a physical or mental disability,
 - (vii) information about the individual's educational, financial, criminal or employment status or history,
 - (viii) the opinions of a person about the individual, and
 - (ix) the individual's personal views or opinions, except where they are about someone else;
- (v) "privacy complaint" means a privacy complaint filed under subsection 73 (1) or (2) or an investigation initiated on the commissioner's own motion under subsection 73 (3);
- (w) "privacy impact assessment" means an assessment that is conducted by a public body as defined under subparagraph (x)(i) to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act;
- (x) "public body" means
- (i) a department created under the *Executive Council Act*, or a branch of the executive government of the province,
 - (ii) a corporation, the ownership of which, or a majority of the shares of which is vested in the Crown,
 - (iii) a corporation, commission or body, the majority of the members of which, or the majority of members of the board of directors of which are appointed by an Act, the Lieutenant-Governor in Council or a minister,
 - (iv) a local public body,
 - (v) the House of Assembly and statutory offices, as defined in the *House of Assembly Accountability, Integrity and Administration Act*, and
 - (vi) a corporation or other entity owned by or created by or for a local government body or group of local government bodies, which has as its primary purpose the management of a local government asset or the discharge of a local government responsibility,
- and includes a body designated for this purpose in the regulations made under section 116, but does not include
- (vii) the constituency office of a member of the House of Assembly wherever located,
 - (viii) the Court of Appeal, the Trial Division, or the Provincial Court, or
 - (ix) a body listed in Schedule B;
- (y) "record" means a record of information in any form, and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium;
- (z) "remuneration" includes salary, wages, overtime pay, bonuses, allowances, honorariums, severance pay, and the aggregate of the contributions of a public body to pension, insurance, health and other benefit plans;

- (aa) "request" means a request made under section 11 for access to a record, including a record containing personal information about the applicant, or correction of personal information, unless the context indicates otherwise;
- (bb) "Schedule B" means the schedule of bodies excluded from the definition of public body; and
- (cc) "third party", in relation to a request for access to a record or for correction of personal information, means a person or group of persons other than
 - (i) the person who made the request, or
 - (ii) a public body.

[2015 cA-1.2 s2; 2017 c10 s3](#)

[Back to Top](#)

Purpose

3. (1) The purpose of this Act is to facilitate democracy through
 - (a) ensuring that citizens have the information required to participate meaningfully in the democratic process;
 - (b) increasing transparency in government and public bodies so that elected officials, officers and employees of public bodies remain accountable; and
 - (c) protecting the privacy of individuals with respect to personal information about themselves held and used by public bodies.
- (2) The purpose is to be achieved by
 - (a) giving the public a right of access to records;
 - (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves;
 - (c) specifying the limited exceptions to the rights of access and correction that are necessary to
 - (i) preserve the ability of government to function efficiently as a cabinet government in a parliamentary democracy,
 - (ii) accommodate established and accepted rights and privileges of others, and
 - (iii) protect from harm the confidential proprietary and other rights of third parties;
 - (d) providing that some discretionary exceptions will not apply where it is clearly demonstrated that the public interest in disclosure outweighs the reason for the exception;
 - (e) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and
 - (f) providing for an oversight agency that
 - (i) is an advocate for access to information and protection of privacy,

- (ii) facilitates timely and user friendly application of this Act,
- (iii) provides independent review of decisions made by public bodies under this Act,
- (iv) provides independent investigation of privacy complaints,
- (v) makes recommendations to government and to public bodies as to actions they might take to better achieve the objectives of this Act, and
- (vi) educates the public and public bodies on all aspects of this Act.

(3) This Act does not replace other procedures for access to information or limit access to information that is not personal information and is available to the public.

[2015 cA-1.2 s3](#)

[Back to Top](#)

Schedule of excluded public bodies

4. When the House of Assembly is not in session, the Lieutenant-Governor in Council, on the recommendation of the House of Assembly Management Commission, may by order amend Schedule B, but the order shall not continue in force beyond the end of the next sitting of the House of Assembly.

[2015 cA-1.2 s4](#)

[Back to Top](#)

Application

5. (1) This Act applies to all records in the custody of or under the control of a public body but does not apply to

- (a) a record in a court file, a record of a judge of the Court of Appeal, Trial Division, or Provincial Court, a judicial administration record or a record relating to support services provided to the judges of those courts;
- (b) a note, communication or draft decision of a person acting in a judicial or quasi-judicial capacity;
- (c) a personal or constituency record of a member of the House of Assembly, that is in the possession or control of the member;
- (d) records of a registered political party or caucus as defined in the *House of Assembly Accountability, Integrity and Administration Act*;
- (e) a personal or constituency record of a minister;
- (f) a record of a question that is to be used on an examination or test;
- (g) a record containing teaching materials or research information of an employee of a post-secondary educational institution;
- (h) material placed in the custody of the Provincial Archives of Newfoundland and Labrador by or for a person other than a public body;
- (i) material placed in the archives of a public body by or for a person other than the public body;

- (j) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed;
 - (k) a record relating to an investigation by the Royal Newfoundland Constabulary if all matters in respect of the investigation have not been completed;
 - (l) a record relating to an investigation by the Royal Newfoundland Constabulary that would reveal the identity of a confidential source of information or reveal information provided by that source with respect to a law enforcement matter; or
 - (m) a record relating to an investigation by the Royal Newfoundland Constabulary in which suspicion of guilt of an identified person is expressed but no charge was ever laid, or relating to prosecutorial consideration of that investigation.
- (2) This Act
- (a) is in addition to existing procedures for access to records or information normally available to the public, including a requirement to pay fees;
 - (b) does not prohibit the transfer, storage or destruction of a record in accordance with an Act of the province or Canada or a by-law or resolution of a local public body;
 - (c) does not limit the information otherwise available by law to a party in a legal proceeding; and
 - (d) does not affect the power of a court or tribunal to compel a witness to testify or to compel the production of a document.

[2015 cA-1.2 s5](#)

[Back to Top](#)

Relationship to Personal Health Information Act

6. (1) Notwithstanding section 5 , but except as provided in sections 92 to 94 , this Act and the regulations shall not apply and the *Personal Health Information Act* and regulations under that Act shall apply where

- (a) a public body is a custodian; and
- (b) the information or record that is in the custody or control of a public body that is a custodian is personal health information.

(2) For the purpose of this section, "custodian" and "personal health information" have the meanings ascribed to them in the *Personal Health Information Act* .

[2015 cA-1.2 s6](#)

[Back to Top](#)

Conflict with other Acts

7. (1) Where there is a conflict between this Act or a regulation made under this Act and another Act or regulation enacted before or after the coming into force of this Act, this Act or the regulation made under it shall prevail.

(2) Notwithstanding subsection (1), where access to a record is prohibited or restricted by, or the right to access a record is provided in a provision designated in Schedule A, that provision shall prevail over this Act or a regulation made under it.

(3) When the House of Assembly is not in session, the Lieutenant-Governor in Council may by order amend Schedule A, but the order shall not continue in force beyond the end of the next sitting of the House of Assembly.

[2015 cA-1.2 s7](#)

PART II ACCESS AND CORRECTION

DIVISION 1 THE REQUEST

[Back to Top](#)

Right of access

8. (1) A person who makes a request under section 11 has a right of access to a record in the custody or under the control of a public body, including a record containing personal information about the applicant.

(2) The right of access to a record does not extend to information excepted from disclosure under this Act, but if it is reasonable to sever that information from the record, an applicant has a right of access to the remainder of the record.

(3) The right of access to a record may be subject to the payment, under section 25, of the costs of reproduction, shipping and locating a record.

[2015 cA-1.2 s8](#)

[Back to Top](#)

Public interest

9. (1) Where the head of a public body may refuse to disclose information to an applicant under a provision listed in subsection (2), that discretionary exception shall not apply where it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception.

(2) Subsection (1) applies to the following sections:

- (a) section 28 (local public body confidences);
- (b) section 29 (policy advice or recommendations);
- (c) subsection 30 (1) (legal advice);
- (d) section 32 (confidential evaluations);
- (e) section 34 (disclosure harmful to intergovernmental relations or negotiations);
- (f) section 35 (disclosure harmful to the financial or economic interests of a public body);
- (g) section 36 (disclosure harmful to conservation); and
- (h) section 38 (disclosure harmful to labour relations interests of public body as employer).

(3) Whether or not a request for access is made, the head of a public body shall, without delay, disclose to the public, to an affected group of people or to an applicant, information about a

risk of significant harm to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.

(4) Subsection (3) applies notwithstanding a provision of this Act.

(5) Before disclosing information under subsection (3), the head of a public body shall, where practicable, give notice of disclosure in the form appropriate in the circumstances to a third party to whom the information relates.

[2015 cA-1.2 s9](#)

[Back to Top](#)

Right to request correction of personal information

10. (1) An individual who believes there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information.

(2) A cost shall not be charged for a request for correction of personal information or for a service in response to that request.

[2015 cA-1.2 s10](#)

[Back to Top](#)

Making a request

11. (1) A person may access a record or seek a correction of personal information by making a request to the public body that the person believes has custody or control of the record or personal information.

(2) A request shall

(a) be in the form set by the minister responsible for this Act;

(b) provide sufficient details about the information requested so that an employee familiar with the records of the public body can identify and locate the record containing the information with reasonable efforts; and

(c) indicate how and in what form the applicant would prefer to access the record.

(3) An applicant may make an oral request for access to a record or correction of personal information where the applicant

(a) has a limited ability to read or write English; or

(b) has a disability or condition that impairs his or her ability to make a request.

(4) A request under subsection (2) may be transmitted by electronic means.

[2015 cA-1.2 s11](#)

[Back to Top](#)

Anonymity

12. (1) The head of a public body shall ensure that the name and type of the applicant is disclosed only to the individual who receives the request on behalf of the public body, the coordinator, the coordinator's assistant and, where necessary, the commissioner.

(2) Subsection (1) does not apply to a request

(a) respecting personal information about the applicant; or

(b) where the name of the applicant is necessary to respond to the request and the applicant has consented to its disclosure.

(3) The disclosure of an applicant's name in a request referred to in subsection (2) shall be limited to the extent necessary to respond to the request.

(4) The limitation on disclosure under subsection (1) applies until the final response to the request is sent to the applicant.

[2015 cA-1.2 s12](#)

[Back to Top](#)

Duty to assist applicant

13. (1) The head of a public body shall make every reasonable effort to assist an applicant in making a request and to respond without delay to an applicant in an open, accurate and complete manner.

(2) The applicant and the head of the public body shall communicate with one another under this Part through the coordinator.

[2015 cA-1.2 s13](#)

[Back to Top](#)

Transferring a request

14. (1) The head of a public body may, upon notifying the applicant in writing, transfer a request to another public body not later than 5 business days after receiving it, where it appears that

(a) the record was produced by or for the other public body; or

(b) the record or personal information is in the custody of or under the control of the other public body.

(2) The head of the public body to which a request is transferred shall respond to the request, and the provisions of this Act shall apply, as if the applicant had originally made the request to and it was received by that public body on the date it was transferred to that public body.

[2015 cA-1.2 s14](#)

[Back to Top](#)

Advisory response

15. (1) The head of a public body shall, not more than 10 business days after receiving a request, provide an advisory response in writing to

(a) advise the applicant as to what will be the final response where

- (i) the record is available and the public body is neither authorized nor required to refuse access to the record under this Act, or
 - (ii) the request for correction of personal information is justified and can be readily made; or
- (b) in other circumstances, advise the applicant of the status of the request.
- (2) An advisory response under paragraph (1)(b) shall inform the applicant about one or more of the following matters, then known:
- (a) a circumstance that may result in the request being refused in full or in part;
 - (b) a cause or other factor that may result in a delay beyond the time period of 20 business days and an estimated length of that delay, for which the head of the public body may seek approval from the commissioner under section 23 to extend the time limit for responding;
 - (c) costs that may be estimated under section 26 to respond to the request;
 - (d) a third party interest in the request; and
 - (e) possible revisions to the request that may facilitate its earlier and less costly response.
- (3) The head of the public body shall, where it is reasonable to do so, provide an applicant with a further advisory response at a later time where an additional circumstance, cause or other factor, costs or a third party interest that may delay receipt of a final response, becomes known.

[2015 cA-1.2 s15](#)

[Back to Top](#)

Time limit for final response

16. (1) The head of a public body shall respond to a request in accordance with section 17 or 18 , without delay and in any event not more than 20 business days after receiving it, unless the time limit for responding is extended under section 23 .

(2) Where the head of a public body fails to respond within the period of 20 business days or an extended period, the head is considered to have refused access to the record or refused the request for correction of personal information.

[2015 cA-1.2 s16](#)

[Back to Top](#)

Content of final response for access

17. (1) In a final response to a request for access to a record, the head of a public body shall inform the applicant in writing

- (a) whether access to the record or part of the record is granted or refused;
- (b) if access to the record or part of the record is granted, where, when and how access will be given; and
- (c) if access to the record or part of the record is refused,

- (i) the reasons for the refusal and the provision of this Act on which the refusal is based, and
 - (ii) that the applicant may file a complaint with the commissioner under section 42 or appeal directly to the Trial Division under section 52 , and advise the applicant of the applicable time limits and how to file a complaint or pursue an appeal.
- (2) Notwithstanding paragraph (1)(c), the head of a public body may in a final response refuse to confirm or deny the existence of
- (a) a record containing information described in section 31 ;
 - (b) a record containing personal information of a third party if disclosure of the existence of the information would be an unreasonable invasion of a third party's personal privacy under section 40 ; or
 - (c) a record that could threaten the health and safety of an individual.

[2015 cA-1.2 s17](#)

[Back to Top](#)

Content of final response for correction of personal information

18. (1) In a final response to a request for correction of personal information, the head of a public body shall inform the applicant in writing

- (a) whether the requested correction has been made; and
 - (b) if the request is refused,
 - (i) the reasons for the refusal,
 - (ii) that the record has been annotated, and
 - (iii) that the applicant may file a complaint with the commissioner under section 42 or appeal directly to the Trial Division under section 52 , and advise the applicant of the applicable time limits and how to file a complaint or pursue an appeal.
- (2) Where no correction is made in response to a request, the head of the public body shall annotate the information with the correction that was requested but not made.
- (3) Where personal information is corrected or annotated under this section, the head of the public body shall notify a public body or a third party to whom that information has been disclosed during the one year period before the correction was requested.
- (4) Where a public body is notified under subsection (3) of a correction or annotation of personal information, the public body shall make the correction or annotation on a record of that information in its custody or under its control.

[2015 cA-1.2 s18](#)

[Back to Top](#)

Third party notification

19. (1) Where the head of a public body intends to grant access to a record or part of a record that the head has reason to believe contains information that might be exempted from disclosure under section 39 or 40 , the head shall make every reasonable effort to notify the third party.

- (2) The time to notify a third party does not suspend the period of time referred to in subsection 16 (1).
- (3) The head of the public body may provide or describe to the third party the content of the record or part of the record for which access is requested.
- (4) The third party may consent to the disclosure of the record or part of the record.
- (5) Where the head of a public body decides to grant access to a record or part of a record and the third party does not consent to the disclosure, the head shall inform the third party in writing
- (a) of the reasons for the decision and the provision of this Act on which the decision is based;
 - (b) of the content of the record or part of the record for which access is to be given;
 - (c) that the applicant will be given access to the record or part of the record unless the third party, not later than 15 business days after the head of the public body informs the third party of this decision, files a complaint with the commissioner under section 42 or appeals directly to the Trial Division under section 53 ; and
 - (d) how to file a complaint or pursue an appeal.
- (6) Where the head of a public body decides to grant access and the third party does not consent to the disclosure, the head shall, in a final response to an applicant, state that the applicant will be given access to the record or part of the record on the completion of the period of 15 business days referred to in subsection (5), unless a third party files a complaint with the commissioner under section 42 or appeals directly to the Trial Division under section 53 .
- (7) The head of the public body shall not give access to the record or part of the record until
- (a) he or she receives confirmation from the third party or the commissioner that the third party has exhausted any recourse under this Act or has decided not to file a complaint or commence an appeal; or
 - (b) a court order has been issued confirming the decision of the public body.
- (8) The head of the public body shall advise the applicant as to the status of a complaint filed or an appeal commenced by the third party.
- (9) The third party and the head of the public body shall communicate with one another under this Part through the coordinator.

[2015 cA-1.2 s19](#)

[Back to Top](#)

Provision of information

- 20.** (1) Where the head of a public body informs an applicant under section 17 that access to a record or part of a record is granted, he or she shall
- (a) give the applicant a copy of the record or part of it, where the applicant requested a copy and the record can reasonably be reproduced; or
 - (b) permit the applicant to examine the record or part of it, where the applicant requested to examine a record or where the record cannot be reasonably reproduced.

(2) Where the requested information is in electronic form in the custody or under the control of a public body, the head of the public body shall produce a record for the applicant where

- (a) it can be produced using the normal computer hardware and software and technical expertise of the public body; and
- (b) producing it would not interfere unreasonably with the operations of the public body.

(3) Where the requested information is information in electronic form that is, or forms part of, a dataset in the custody or under the control of a public body, the head of the public body shall produce the information for the applicant in an electronic form that is capable of re-use where

- (a) it can be produced using the normal computer hardware and software and technical expertise of the public body;
- (b) producing it would not interfere unreasonably with the operations of the public body; and
- (c) it is reasonably practicable to do so.

(4) Where information that is, or forms part of, a dataset is produced, the head of the public body shall make it available for re-use in accordance with the terms of a licence that may be applicable to the dataset.

(5) Where a record exists, but not in the form requested by the applicant, the head of the public body may, in consultation with the applicant, create a record in the form requested where the head is of the opinion that it would be simpler or less costly for the public body to do so.

[2015 cA-1.2 s20](#)

[Back to Top](#)

Disregarding a request

21. (1) The head of a public body may, not later than 5 business days after receiving a request, apply to the commissioner for approval to disregard the request where the head is of the opinion that

- (a) the request would unreasonably interfere with the operations of the public body;
- (b) the request is for information already provided to the applicant; or
- (c) the request would amount to an abuse of the right to make a request because it is
 - (i) trivial, frivolous or vexatious,
 - (ii) unduly repetitive or systematic,
 - (iii) excessively broad or incomprehensible, or
 - (iv) otherwise made in bad faith.

(2) The commissioner shall, without delay and in any event not later than 3 business days after receiving an application, decide to approve or disapprove the application.

(3) The time to make an application and receive a decision from the commissioner does not suspend the period of time referred to in subsection 16 (1).

(4) Where the commissioner does not approve the application, the head of the public body shall respond to the request in the manner required by this Act.

(5) Where the commissioner approves the application, the head of a public body who refuses to give access to a record or correct personal information under this section shall notify the person who made the request.

(6) The notice shall contain the following information:

(a) that the request is refused because the head of the public body is of the opinion that the request falls under subsection (1) and of the reasons for the refusal;

(b) that the commissioner has approved the decision of the head of a public body to disregard the request; and

(c) that the person who made the request may appeal the decision of the head of the public body to the Trial Division under subsection 52 (1).

[2015 cA-1.2 s21](#)

[Back to Top](#)

Published material

22. (1) The head of a public body may refuse to disclose a record or part of a record that

(a) is published and is available to the public whether without cost or for purchase; or

(b) is to be published or released to the public within 30 business days after the applicant's request is received.

(2) The head of a public body shall notify an applicant of the publication or release of information that the head has refused to give access to under paragraph (1)(b).

(3) Where the information is not published or released within 30 business days after the applicant's request is received, the head of the public body shall reconsider the request as if it were a new request received on the last day of that period, and access may not be refused under paragraph (1)(b).

[2015 cA-1.2 s22](#)

[Back to Top](#)

Extension of time limit

23. (1) The head of a public body may, not later than 15 business days after receiving a request, apply to the commissioner to extend the time for responding to the request.

(2) The commissioner may approve an application for an extension of time where the commissioner considers that it is necessary and reasonable to do so in the circumstances, for the number of business days the commissioner considers appropriate.

(3) The commissioner shall, without delay and not later than 3 business days after receiving an application, decide to approve or disapprove the application.

(4) The time to make an application and receive a decision from the commissioner does not suspend the period of time referred to in subsection 16 (1).

(5) Where the commissioner does not approve the application, the head of the public body shall respond to the request under subsection 16 (1) without delay and in any event not later than 20 business days after receiving the request.

(6) Where the commissioner approves the application and the time limit for responding is extended, the head of the public body shall, without delay, notify the applicant in writing

- (a) of the reason for the extension;
- (b) that the commissioner has authorized the extension; and
- (c) when a response can be expected.

[2015 cA-1.2 s23](#)

[Back to Top](#)

Extraordinary circumstances

24. (1) The head of a public body, an applicant or a third party may, in extraordinary circumstances, apply to the commissioner to vary a procedure, including a time limit imposed under a procedure, in this Part.

(2) Where the commissioner considers that extraordinary circumstances exist and it is necessary and reasonable to do so, the commissioner may vary the procedure as requested or in another manner that the commissioner considers appropriate.

(3) The commissioner shall, without delay and not later than 3 business days after receiving an application, make a decision to vary or not vary the procedure.

(4) The time to make an application and receive a decision from the commissioner does not suspend the period of time referred to in subsection 16 (1).

(5) Where the commissioner decides to vary a procedure upon an application of a head of a public body or a third party, the head shall notify the applicant in writing

- (a) of the reason for the procedure being varied; and
- (b) that the commissioner has authorized the variance.

(6) Where the commissioner decides to vary a procedure upon an application of an applicant to a request, the commissioner shall notify the head of the public body of the variance.

(7) An application cannot be made to vary a procedure for which the commissioner is responsible under this Part.

[2015 cA-1.2 s24](#)

[Back to Top](#)

Costs

25. (1) The head of a public body shall not charge an applicant for making an application for access to a record or for the services of identifying, retrieving, reviewing, severing or redacting a record.

(2) The head of a public body may charge an applicant a modest cost for locating a record only, after

- (a) the first 10 hours of locating the record, where the request is made to a local government body; or
 - (b) the first 15 hours of locating the record, where the request is made to another public body.
- (3) The head of a public body may require an applicant to pay
- (a) a modest cost for copying or printing a record, where the record is to be provided in hard copy form;
 - (b) the actual cost of reproducing or providing a record that cannot be reproduced or printed on conventional equipment then in use by the public body; and
 - (c) the actual cost of shipping a record using the method chosen by the applicant.
- (4) Notwithstanding subsections (2) and (3), the head of the public body shall not charge an applicant a cost for a service in response to a request for access to the personal information of the applicant.
- (5) The cost charged for services under this section shall not exceed either
- (a) the estimate given to the applicant under section 26 ; or
 - (b) the actual cost of the services.
- (6) The minister responsible for the administration of this Act may set the amount of a cost that may be charged under this section.

[2015 cA-1.2 s25](#)

[Back to Top](#)

Estimate and waiver of costs

26. (1) Where an applicant is to be charged a cost under section 25 , the head of the public body shall give the applicant an estimate of the total cost before providing the services.

(2) The applicant has 20 business days from the day the estimate is sent to accept the estimate or modify the request in order to change the amount of the cost, after which time the applicant is considered to have abandoned the request, unless the applicant applies for a waiver of all or part of the costs or applies to the commissioner to revise the estimate.

(3) The head of a public body may, on receipt of an application from an applicant, waive the payment of all or part of the costs payable under section 25 where the head is satisfied that

- (a) payment would impose an unreasonable financial hardship on the applicant; or
- (b) it would be in the public interest to disclose the record.

(4) Within the time period of 20 business days referred to in subsection (2), the head of the public body shall inform the applicant in writing as to the head's decision about waiving all or part of the costs and the applicant shall either accept the decision or apply to the commissioner to review the decision.

(5) Where an applicant applies to the commissioner to revise an estimate of costs or to review a decision of the head of the public body not to waive all or part of the costs, the time period

of 20 business days referred to in subsection (2) is suspended until the application has been considered by the commissioner.

(6) Where an estimate is given to an applicant under this section, the time within which the head of the public body is required to respond to the request is suspended until the applicant notifies the head to proceed with the request.

(7) On an application to revise an estimate, the commissioner may

(a) where the commissioner considers that it is necessary and reasonable to do so in the circumstances, revise the estimate and set the appropriate amount to be charged and a refund, if any; or

(b) confirm the decision of the head of the public body.

(8) On an application to review the decision of the head of the public body not to waive the payment of all or part of the costs, the commissioner may

(a) where the commissioner is satisfied that paragraph (3)(a) or (b) is applicable, waive the payment of the costs or part of the costs in the manner and in the amount that the commissioner considers appropriate; or

(b) confirm the decision of the head of the public body.

(9) The head of the public body shall comply with a decision of the commissioner under this section.

(10) Where an estimate of costs has been provided to an applicant, the head of a public body may require the applicant to pay 50% of the cost before commencing the services, with the remainder to be paid upon completion of the services.

[2015 cA-1.2 s26](#)

DIVISION 2 EXCEPTIONS TO ACCESS

[Back to Top](#)

Cabinet confidences

27. (1) In this section, "cabinet record" means

(a) advice, recommendations or policy considerations submitted or prepared for submission to the Cabinet;

(b) draft legislation or regulations submitted or prepared for submission to the Cabinet;

(c) a memorandum, the purpose of which is to present proposals or recommendations to the Cabinet;

(d) a discussion paper, policy analysis, proposal, advice or briefing material prepared for Cabinet, excluding the sections of these records that are factual or background material;

(e) an agenda, minute or other record of Cabinet recording deliberations or decisions of the Cabinet;

- (f) a record used for or which reflects communications or discussions among ministers on matters relating to the making of government decisions or the formulation of government policy;
- (g) a record created for or by a minister for the purpose of briefing that minister on a matter for the Cabinet;
- (h) a record created during the process of developing or preparing a submission for the Cabinet; and
- (i) that portion of a record which contains information about the contents of a record within a class of information referred to in paragraphs (a) to (h).

(2) The head of a public body shall refuse to disclose to an applicant

- (a) a cabinet record; or
- (b) information in a record other than a cabinet record that would reveal the substance of deliberations of Cabinet.

(3) Notwithstanding subsection (2), the Clerk of the Executive Council may disclose a cabinet record or information that would reveal the substance of deliberations of Cabinet where the Clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.

(4) Subsections (1) and (2) do not apply to

- (a) information in a record that has been in existence for 20 years or more; or
- (b) information in a record of a decision made by the Cabinet on an appeal under an Act.

[2015 cA-1.2 s27](#)

[Back to Top](#)

Local public body confidences

28. (1) The head of a local public body may refuse to disclose to an applicant information that would reveal

- (a) a draft of a resolution, by-law or other legal instrument by which the local public body acts;
- (b) a draft of a private Bill; or
- (c) the substance of deliberations of a meeting of its elected officials or governing body or a committee of its elected officials or governing body, where an Act authorizes the holding of a meeting in the absence of the public.

(2) Subsection (1) does not apply where

- (a) the draft of a resolution, by-law or other legal instrument, a private Bill or the subject matter of deliberations has been considered, other than incidentally, in a meeting open to the public; or
- (b) the information referred to in subsection (1) is in a record that has been in existence for 15 years or more.

[2015 cA-1.2 s28](#)

[Back to Top](#)

Policy advice or recommendations

29. (1) The head of a public body may refuse to disclose to an applicant information that would reveal

- (a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or minister;
- (b) the contents of a formal research report or audit report that in the opinion of the head of the public body is incomplete and in respect of which a request or order for completion has been made by the head within 65 business days of delivery of the report; or
- (c) draft legislation or regulations.

(2) The head of a public body shall not refuse to disclose under subsection (1)

- (a) factual material;
- (b) a public opinion poll;
- (c) a statistical survey;
- (d) an appraisal;
- (e) an environmental impact statement or similar information;
- (f) a final report or final audit on the performance or efficiency of a public body or on any of its programs or policies;
- (g) a consumer test report or a report of a test carried out on a product to test equipment of the public body;
- (h) a feasibility or technical study, including a cost estimate, relating to a policy or project of the public body;
- (i) a report on the results of field research undertaken before a policy proposal is formulated;
- (j) a report of an external task force, committee, council or similar body that has been established to consider a matter and make a report or recommendations to a public body;
- (k) a plan or proposal to establish a new program or to change a program, if the plan or proposal has been approved or rejected by the head of the public body;
- (l) information that the head of the public body has cited publicly as the basis for making a decision or formulating a policy; or
- (m) a decision, including reasons, that is made in the exercise of a discretionary power or an adjudicative function and that affects the rights of the applicant.

(3) Subsection (1) does not apply to information in a record that has been in existence for 15 years or more.

[2015 cA-1.2 s29](#)

[Back to Top](#)

Legal advice

30. (1) The head of a public body may refuse to disclose to an applicant information

- (a) that is subject to solicitor and client privilege or litigation privilege of a public body; or
- (b) that would disclose legal opinions provided to a public body by a law officer of the Crown.

(2) The head of a public body shall refuse to disclose to an applicant information that is subject to solicitor and client privilege or litigation privilege of a person other than a public body.

[2015 cA-1.2 s30](#)

[Back to Top](#)

Disclosure harmful to law enforcement

31. (1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to

- (a) interfere with or harm a law enforcement matter;
- (b) prejudice the defence of Canada or of a foreign state allied to or associated with Canada or harm the detection, prevention or suppression of espionage, sabotage or terrorism;
- (c) reveal investigative techniques and procedures currently used, or likely to be used, in law enforcement;
- (d) reveal the identity of a confidential source of law enforcement information or reveal information provided by that source with respect to a law enforcement matter;
- (e) reveal law enforcement intelligence information;
- (f) endanger the life or physical safety of a law enforcement officer or another person;
- (g) reveal information relating to or used in the exercise of prosecutorial discretion;
- (h) deprive a person of the right to a fair trial or impartial adjudication;
- (i) reveal a record that has been confiscated from a person by a peace officer in accordance with an Act or regulation;
- (j) facilitate the escape from custody of a person who is under lawful detention;
- (k) facilitate the commission or tend to impede the detection of an offence under an Act or regulation of the province or Canada ;
- (l) reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;
- (m) reveal technical information about weapons used or that may be used in law enforcement;
- (n) adversely affect the detection, investigation, prevention or prosecution of an offence or the security of a centre of lawful detention;

- (o) reveal information in a correctional record supplied, implicitly or explicitly, in confidence; or
 - (p) harm the conduct of existing or imminent legal proceedings.
- (2) The head of a public body may refuse to disclose information to an applicant if the information
- (a) is in a law enforcement record and the disclosure would be an offence under an Act of Parliament;
 - (b) is in a law enforcement record and the disclosure could reasonably be expected to expose to civil liability the author of the record or a person who has been quoted or paraphrased in the record; or
 - (c) is about the history, supervision or release of a person who is in custody or under supervision and the disclosure could reasonably be expected to harm the proper custody or supervision of that person.
- (3) The head of a public body shall not refuse to disclose under this section
- (a) a report prepared in the course of routine inspections by an agency that is authorized to enforce compliance with an Act; or
 - (b) a report, including statistical analysis, on the degree of success achieved in a law enforcement program unless disclosure of the report could reasonably be expected to interfere with or harm the matters referred to in subsection (1) or (2); or
 - (c) statistical information on decisions to approve or not to approve prosecutions.

[2015 cA-1.2 s31](#)

[Back to Top](#)

Confidential evaluations

32. The head of a public body may refuse to disclose to an applicant personal information that is evaluative or opinion material, provided explicitly or implicitly in confidence, and compiled for the purpose of

- (a) determining suitability, eligibility or qualifications for employment or for the awarding of contracts or other benefits by a public body;
- (b) determining suitability, eligibility or qualifications for admission to an academic program of an educational body;
- (c) determining suitability, eligibility or qualifications for the granting of tenure at a post-secondary educational body;
- (d) determining suitability, eligibility or qualifications for an honour or award to recognize outstanding achievement or distinguished service; or
- (e) assessing the teaching materials or research of an employee of a post-secondary educational body or of a person associated with an educational body.

[2015 cA-1.2 s32](#)

[Back to Top](#)

Information from a workplace investigation

33. (1) For the purpose of this section

- (a) "harassment" means comments or conduct which are abusive, offensive, demeaning or vexatious that are known, or ought reasonably to be known, to be unwelcome and which may be intended or unintended;
- (b) "party" means a complainant, respondent or a witness who provided a statement to an investigator conducting a workplace investigation; and
- (c) "workplace investigation" means an investigation related to
 - (i) the conduct of an employee in the workplace,
 - (ii) harassment, or
 - (iii) events related to the interaction of an employee in the public body's workplace with another employee or a member of the public

which may give rise to progressive discipline or corrective action by the public body employer.

(2) The head of a public body shall refuse to disclose to an applicant all relevant information created or gathered for the purpose of a workplace investigation.

(3) The head of a public body shall disclose to an applicant who is a party to a workplace investigation the information referred to in subsection (2).

(4) Notwithstanding subsection (3), where a party referred to in that subsection is a witness in a workplace investigation, the head of a public body shall disclose only the information referred to in subsection (2) which relates to the witness' statements provided in the course of the investigation.

[2015 cA-1.2 s33](#)

[Back to Top](#)

Disclosure harmful to intergovernmental relations or negotiations

34. (1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

- (a) harm the conduct by the government of the province of relations between that government and the following or their agencies:
 - (i) the government of Canada or a province,
 - (ii) the council of a local government body,
 - (iii) the government of a foreign state,
 - (iv) an international organization of states, or
 - (v) the Nunatsiavut Government; or
- (b) reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies.

(2) The head of a public body shall not disclose information referred to in subsection (1) without the consent of

- (a) the Attorney General, for law enforcement information; or
- (b) the Lieutenant-Governor in Council, for any other type of information.

(3) Subsection (1) does not apply to information that is in a record that has been in existence for 15 years or more unless the information is law enforcement information.

[2015 cA-1.2 s34](#)

[Back to Top](#)

Disclosure harmful to the financial or economic interests of a public body

35. (1) The head of a public body may refuse to disclose to an applicant information which could reasonably be expected to disclose

- (a) trade secrets of a public body or the government of the province;
- (b) financial, commercial, scientific or technical information that belongs to a public body or to the government of the province and that has, or is reasonably likely to have, monetary value;
- (c) plans that relate to the management of personnel of or the administration of a public body and that have not yet been implemented or made public;
- (d) information, the disclosure of which could reasonably be expected to result in the premature disclosure of a proposal or project or in significant loss or gain to a third party;
- (e) scientific or technical information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee of priority of publication;
- (f) positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the government of the province or a public body, or considerations which relate to those negotiations;
- (g) information, the disclosure of which could reasonably be expected to prejudice the financial or economic interest of the government of the province or a public body; or
- (h) information, the disclosure of which could reasonably be expected to be injurious to the ability of the government of the province to manage the economy of the province.

(2) The head of a public body shall not refuse to disclose under subsection (1) the results of product or environmental testing carried out by or for that public body, unless the testing was done

- (a) for a fee as a service to a person or a group of persons other than the public body; or
- (b) for the purpose of developing methods of testing.

[2015 cA-1.2 s35](#)

[Back to Top](#)

Disclosure harmful to conservation

36. The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to result in damage to, or interfere with the conservation of

- (a) fossil sites, natural sites or sites that have an anthropological or heritage value;
- (b) an endangered, threatened or vulnerable species, sub-species or a population of a species; or
- (c) a rare or endangered living resource.

[2015 cA-1.2 s36](#)

[Back to Top](#)

Disclosure harmful to individual or public safety

37. (1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, where the disclosure could reasonably be expected to

- (a) threaten the safety or mental or physical health of a person other than the applicant; or
- (b) interfere with public safety.

(2) The head of a public body may refuse to disclose to an applicant personal information about the applicant if the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's safety or mental or physical health.

[2015 cA-1.2 s37](#)

[Back to Top](#)

Disclosure harmful to labour relations interests of public body as employer

38. (1) The head of a public body may refuse to disclose to an applicant information that would reveal

- (a) labour relations information of the public body as an employer that is prepared or supplied, implicitly or explicitly, in confidence, and is treated consistently as confidential information by the public body as an employer; or
- (b) labour relations information the disclosure of which could reasonably be expected to
 - (i) harm the competitive position of the public body as an employer or interfere with the negotiating position of the public body as an employer,
 - (ii) result in significant financial loss or gain to the public body as an employer, or
 - (iii) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer, staff relations specialist or other person or body appointed to resolve or inquire into a labour relations dispute, including information or records prepared by or for the public body in contemplation of litigation or arbitration or in contemplation of a settlement offer.

(2) Subsection (1) does not apply where the information is in a record that is in the custody or control of the Provincial Archives of Newfoundland and Labrador or the archives of a public body and that has been in existence for 50 years or more.

[2015 cA-1.2 s38](#)

[Back to Top](#)

Disclosure harmful to business interests of a third party

- 39.** (1) The head of a public body shall refuse to disclose to an applicant information
- (a) that would reveal
 - (i) trade secrets of a third party, or
 - (ii) commercial, financial, labour relations, scientific or technical information of a third party;
 - (b) that is supplied, implicitly or explicitly, in confidence; and
 - (c) the disclosure of which could reasonably be expected to
 - (i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,
 - (ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
 - (iii) result in undue financial loss or gain to any person, or
 - (iv) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

(2) The head of a public body shall refuse to disclose to an applicant information that was obtained on a tax return, gathered for the purpose of determining tax liability or collecting a tax, or royalty information submitted on royalty returns, except where that information is non-identifying aggregate royalty information.

- (3) Subsections (1) and (2) do not apply where
- (a) the third party consents to the disclosure; or
 - (b) the information is in a record that is in the custody or control of the Provincial Archives of Newfoundland and Labrador or the archives of a public body and that has been in existence for 50 years or more.

[2015 cA-1.2 s39](#)

[Back to Top](#)

Disclosure harmful to personal privacy

40. (1) The head of a public body shall refuse to disclose personal information to an applicant where the disclosure would be an unreasonable invasion of a third party's personal privacy.

(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy where

- (a) the applicant is the individual to whom the information relates;
- (b) the third party to whom the information relates has, in writing, consented to or requested the disclosure;

- (c) there are compelling circumstances affecting a person's health or safety and notice of disclosure is given in the form appropriate in the circumstances to the third party to whom the information relates;
 - (d) an Act or regulation of the province or of Canada authorizes the disclosure;
 - (e) the disclosure is for a research or statistical purpose and is in accordance with section 70 ;
 - (f) the information is about a third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff;
 - (g) the disclosure reveals financial and other details of a contract to supply goods or services to a public body;
 - (h) the disclosure reveals the opinions or views of a third party given in the course of performing services for a public body, except where they are given in respect of another individual;
 - (i) public access to the information is provided under the *Financial Administration Act* ;
 - (j) the information is about expenses incurred by a third party while travelling at the expense of a public body;
 - (k) the disclosure reveals details of a licence, permit or a similar discretionary benefit granted to a third party by a public body, not including personal information supplied in support of the application for the benefit;
 - (l) the disclosure reveals details of a discretionary benefit of a financial nature granted to a third party by a public body, not including
 - (i) personal information that is supplied in support of the application for the benefit, or
 - (ii) personal information that relates to eligibility for income and employment support under the *Income and Employment Support Act* or to the determination of income or employment support levels; or
 - (m) the disclosure is not contrary to the public interest as described in subsection (3) and reveals only the following personal information about a third party:
 - (i) attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or
 - (ii) receipt of an honour or award granted by or through a public body.
- (3) The disclosure of personal information under paragraph (2)(m) is an unreasonable invasion of personal privacy where the third party whom the information is about has requested that the information not be disclosed.
- (4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy where
- (a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;

- (b) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation;
 - (c) the personal information relates to employment or educational history;
 - (d) the personal information was collected on a tax return or gathered for the purpose of collecting a tax;
 - (e) the personal information consists of an individual's bank account information or credit card information;
 - (f) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations;
 - (g) the personal information consists of the third party's name where
 - (i) it appears with other personal information about the third party, or
 - (ii) the disclosure of the name itself would reveal personal information about the third party; or
 - (h) the personal information indicates the third party's racial or ethnic origin or religious or political beliefs or associations.
- (5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether
- (a) the disclosure is desirable for the purpose of subjecting the activities of the province or a public body to public scrutiny;
 - (b) the disclosure is likely to promote public health and safety or the protection of the environment;
 - (c) the personal information is relevant to a fair determination of the applicant's rights;
 - (d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;
 - (e) the third party will be exposed unfairly to financial or other harm;
 - (f) the personal information has been supplied in confidence;
 - (g) the personal information is likely to be inaccurate or unreliable;
 - (h) the disclosure may unfairly damage the reputation of a person referred to in the record requested by the applicant;
 - (i) the personal information was originally provided to the applicant; and
 - (j) the information is about a deceased person and, if so, whether the length of time the person has been deceased indicates the disclosure is not an unreasonable invasion of the deceased person's personal privacy.

[2015 cA-1.2 s40](#)

[Back to Top](#)

Disclosure of House of Assembly service and statutory office records

41. The Speaker of the House of Assembly, the officer responsible for a statutory office, or the head of a public body shall refuse to disclose to an applicant information

- (a) where its non-disclosure is required for the purpose of avoiding an infringement of the privileges of the House of Assembly or a member of the House of Assembly;
- (b) that is advice or a recommendation given to the Speaker or the Clerk of the House of Assembly or the House of Assembly Management Commission that is not required by law to be disclosed or placed in the minutes of the House of Assembly Management Commission; or
- (c) in the case of a statutory office as defined in the *House of Assembly Accountability, Integrity and Administration Act*, records connected with the investigatory functions of the statutory office.

[2015 cA-1.2 s41](#)

DIVISION 3 COMPLAINT

[Back to Top](#)

Access or correction complaint

42. (1) A person who makes a request under this Act for access to a record or for correction of personal information may file a complaint with the commissioner respecting a decision, act or failure to act of the head of the public body that relates to the request.

(2) A complaint under subsection (1) shall be filed in writing not later than 15 business days

- (a) after the applicant is notified of the decision of the head of the public body, or the date of the act or failure to act; or
- (b) after the date the head of the public body is considered to have refused the request under subsection 16 (2).

(3) A third party informed under section 19 of a decision of the head of a public body to grant access to a record or part of a record in response to a request may file a complaint with the commissioner respecting that decision.

(4) A complaint under subsection (3) shall be filed in writing not later than 15 business days after the third party is informed of the decision of the head of the public body.

(5) The commissioner may allow a longer time period for the filing of a complaint under this section.

(6) A person or third party who has appealed directly to the Trial Division under subsection 52 (1) or 53 (1) shall not file a complaint with the commissioner.

(7) The commissioner shall refuse to investigate a complaint where an appeal has been commenced in the Trial Division.

(8) A complaint shall not be filed under this section with respect to

- (a) a request that is disregarded under section 21 ;

- (b) a decision respecting an extension of time under section 23 ;
 - (c) a variation of a procedure under section 24 ; or
 - (d) an estimate of costs or a decision not to waive a cost under section 26 .
- (9) The commissioner shall provide a copy of the complaint to the head of the public body concerned.

[2015 cA-1.2 s42](#)

[Back to Top](#)

Burden of proof

43. (1) On an investigation of a complaint from a decision to refuse access to a record or part of a record, the burden is on the head of a public body to prove that the applicant has no right of access to the record or part of the record.

(2) On an investigation of a complaint from a decision to give an applicant access to a record or part of a record containing personal information that relates to a third party, the burden is on the head of a public body to prove that the disclosure of the information would not be contrary to this Act or the regulations.

(3) On an investigation of a complaint from a decision to give an applicant access to a record or part of a record containing information, other than personal information, that relates to a third party, the burden is on the third party to prove that the applicant has no right of access to the record or part of the record.

[2015 cA-1.2 s43](#)

[Back to Top](#)

Investigation

44. (1) The commissioner shall notify the parties to the complaint and advise them that they have 10 business days from the date of notification to make representations to the commissioner.

(2) The parties to the complaint may, not later than 10 business days after notification of the complaint, make a representation to the commissioner in accordance with section 96 .

(3) The commissioner may take additional steps that he or she considers appropriate to resolve the complaint informally to the satisfaction of the parties and in a manner consistent with this Act.

(4) Where the commissioner is unable to informally resolve the complaint within 30 business days of receipt of the complaint, the commissioner shall conduct a formal investigation of the subject matter of the complaint where he or she is satisfied that there are reasonable grounds to do so.

(5) Notwithstanding subsection (4), the commissioner may extend the informal resolution process for a maximum of 20 business days where a written request is received from each party to continue the informal resolution process.

(6) The commissioner shall not extend the informal resolution process beyond the date that is 50 business days after receipt of the complaint.

(7) Where the commissioner has 5 active complaints from the same applicant that deal with similar or related records, the commissioner may hold an additional complaint in abeyance and not commence an investigation until one of the 5 active complaints is resolved.

[2015 cA-1.2 s44](#)

[Back to Top](#)

Authority of commissioner not to investigate a complaint

45. (1) The commissioner may, at any stage of an investigation, refuse to investigate a complaint where he or she is satisfied that

- (a) the head of a public body has responded adequately to the complaint;
 - (b) the complaint has been or could be more appropriately dealt with by a procedure or proceeding other than a complaint under this Act;
 - (c) the length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was filed is such that an investigation under this Part would be likely to result in undue prejudice to a person or that a report would not serve a useful purpose; or
 - (d) the complaint is trivial, frivolous, vexatious or is made in bad faith.
- (2) Where the commissioner refuses to investigate a complaint, he or she shall
- (a) give notice of that refusal, together with reasons, to the person who made the complaint;
 - (b) advise the person of the right to appeal to the Trial Division under subsection 52 (3) or 53 (3) the decision of the head of the public body that relates to the request; and
 - (c) advise the person of the applicable time limit and how to pursue an appeal.

[2015 cA-1.2 s45](#)

[Back to Top](#)

Time limit for formal investigation

46. (1) The commissioner shall complete a formal investigation and make a report under section 48 within 65 business days of receiving the complaint, whether or not the time for the informal resolution process has been extended.

(2) The commissioner may, in extraordinary circumstances, apply to a judge of the Trial Division for an order to extend the period of time under subsection (1).

[2015 cA-1.2 s46](#)

[Back to Top](#)

Recommendations

47. On completing an investigation, the commissioner may recommend that

- (a) the head of the public body grant or refuse access to the record or part of the record;
- (b) the head of the public body reconsider its decision to refuse access to the record or part of the record;
- (c) the head of the public body either make or not make the requested correction to personal information; and

- (d) other improvements for access to information be made within the public body.

[2015 cA-1.2 s47](#)

[Back to Top](#)

Report

48. (1) On completing an investigation, the commissioner shall

- (a) prepare a report containing the commissioner's findings and, where appropriate, his or her recommendations and the reasons for those recommendations; and
- (b) send a copy of the report to the person who filed the complaint, the head of the public body concerned and a third party who was notified under section 44 .

(2) The report shall include information respecting the obligation of the head of the public body to notify the parties of the head's response to the recommendation of the commissioner within 10 business days of receipt of the recommendation.

[2015 cA-1.2 s48](#)

[Back to Top](#)

Response of public body

49. (1) The head of a public body shall, not later than 10 business days after receiving a recommendation of the commissioner,

- (a) decide whether or not to comply with the recommendation in whole or in part; and
- (b) give written notice of his or her decision to the commissioner and a person who was sent a copy of the report.

(2) Where the head of the public body does not give written notice within the time required by subsection (1), the head of the public body is considered to have agreed to comply with the recommendation of the commissioner.

(3) The written notice shall include notice of the right

- (a) of an applicant or third party to appeal under section 54 to the Trial Division and of the time limit for an appeal; or
- (b) of the commissioner to file an order with the Trial Division in one of the circumstances referred to in subsection 51 (1).

[2015 cA-1.2 s49](#)

[Back to Top](#)

Head of public body seeks declaration in court

50. (1) This section applies to a recommendation of the commissioner under section 47 that the head of the public body

- (a) grant the applicant access to the record or part of the record; or
- (b) make the requested correction to personal information.

(2) Where the head of the public body decides not to comply with a recommendation of the commissioner referred to in subsection (1) in whole or in part, the head shall, not later than 10 business days after receipt of that recommendation, apply to the Trial Division for a declaration that the public body is not required to comply with that recommendation because

- (a) the head of the public body is authorized under this Part to refuse access to the record or part of the record, and, where applicable, it has not been clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception;
- (b) the head of the public body is required under this Part to refuse access to the record or part of the record; or
- (c) the decision of the head of the public body not to make the requested correction to personal information is in accordance with this Act or the regulations.

(3) The head shall, within the time frame referred to in subsection (2), serve a copy of the application for a declaration on the commissioner, the minister responsible for the administration of this Act, and a person who was sent a copy of the commissioner's report.

(4) The commissioner, the minister responsible for this Act, or a person who was sent a copy of the commissioner's report may intervene in an application for a declaration by filing a notice to that effect with the Trial Division.

(5) Sections 57 to 60 apply, with the necessary modifications, to an application by the head of a public body to the Trial Division for a declaration.

[2015 cA-1.2 s50](#)

[Back to Top](#)

Filing an order with the Trial Division

51. (1) The commissioner may prepare and file an order with the Trial Division where

- (a) the head of the public body agrees or is considered to have agreed under section 49 to comply with a recommendation of the commissioner referred to in subsection 50 (1) in whole or in part but fails to do so within 15 business days after receipt of the commissioner's recommendation; or
 - (b) the head of the public body fails to apply under section 50 to the Trial Division for a declaration.
- (2) The order shall be limited to a direction to the head of the public body either
- (a) to grant the applicant access to the record or part of the record; or
 - (b) to make the requested correction to personal information.

(3) An order shall not be filed with the Trial Division until the later of the time periods referred to in paragraph (1)(a) and section 54 has passed.

(4) An order shall not be filed with the Trial Division under this section if the applicant or third party has commenced an appeal in the Trial Division under section 54 .

(5) Where an order is filed with the Trial Division, it is enforceable against the public body as if it were a judgment or order made by the court.

[2015 cA-1.2 s51](#)

**DIVISION 4
APPEAL TO THE TRIAL DIVISION**

[Back to Top](#)

Direct appeal to Trial Division by an applicant

52. (1) Where an applicant has made a request to a public body for access to a record or correction of personal information and has not filed a complaint with the commissioner under section 42, the applicant may appeal the decision, act or failure to act of the head of the public body that relates to the request directly to the Trial Division.

(2) An appeal shall be commenced under subsection (1) not later than 15 business days

(a) after the applicant is notified of the decision of the head of the public body, or the date of the act or failure to act; or

(b) after the date the head of the public body is considered to have refused the request under subsection 16 (2).

(3) Where an applicant has filed a complaint with the commissioner under section 42 and the commissioner has refused to investigate the complaint, the applicant may commence an appeal in the Trial Division of the decision, act or failure to act of the head of the public body that relates to the request for access to a record or for correction of personal information.

(4) An appeal shall be commenced under subsection (3) not later than 15 business days after the applicant is notified of the commissioner's refusal under subsection 45 (2).

[2015 cA-1.2 s52](#)

[Back to Top](#)

Direct appeal to Trial Division by a third party

53. (1) A third party informed under section 19 of a decision of the head of a public body to grant access to a record or part of a record in response to a request may appeal the decision directly to the Trial Division.

(2) An appeal shall be commenced under subsection (1) not later than 15 business days after the third party is informed of the decision of the head of the public body.

(3) Where a third party has filed a complaint with the commissioner under section 42 and the commissioner has refused to investigate the complaint, the third party may commence an appeal in the Trial Division of the decision of the head of the public body to grant access in response to a request.

(4) An appeal shall be commenced under subsection (3) not later than 15 business days after the third party is notified of the commissioner's refusal under subsection 45 (2).

[2015 cA-1.2 s53](#)

[Back to Top](#)

Appeal of public body decision after receipt of commissioner's recommendation

54. An applicant or a third party may, not later than 10 business days after receipt of a decision of the head of the public body under section 49, commence an appeal in the Trial Division of the head's decision to

- (a) grant or refuse access to the record or part of the record; or
- (b) not make the requested correction to personal information.

[2015 cA-1.2 s54](#)

[Back to Top](#)

No right of appeal

55. An appeal does not lie against

- (a) a decision respecting an extension of time under section 23 ;
- (b) a variation of a procedure under section 24 ; or
- (c) an estimate of costs or a decision not to waive a cost under section 26 .

[2015 cA-1.2 s55](#)

[Back to Top](#)

Procedure on appeal

56. (1) Where a person appeals a decision of the head of a public body, the notice of appeal shall name the head of the public body involved as the respondent.

(2) A copy of the notice of appeal shall be served by the appellant on the commissioner and the minister responsible for this Act.

(3) The minister responsible for this Act, the commissioner, the applicant or a third party may intervene as a party to an appeal under this Division by filing a notice to that effect with the Trial Division.

(4) Notwithstanding subsection (3), the commissioner shall not intervene as a party to an appeal of

- (a) a decision of the head of the public body under section 21 to disregard a request; or
- (b) a decision, act or failure to act of the head of a public body in respect of which the commissioner has refused under section 45 to investigate a complaint.

(5) The head of a public body who has refused access to a record or part of it shall, on receipt of a notice of appeal by an applicant, make reasonable efforts to give written notice of the appeal to a third party who

- (a) was notified of the request for access under section 19 ; or
- (b) would have been notified under section 19 if the head had intended to give access to the record or part of the record.

(6) Where an appeal is brought by a third party, the head of the public body shall give written notice of the appeal to the applicant.

(7) The record for the appeal shall be prepared by the head of the public body named as the respondent in the appeal.

[2015 cA-1.2 s56](#)

[Back to Top](#)

Practice and procedure

57. The practice and procedure under the *Rules of the Supreme Court, 1986* providing for an expedited trial, or such adaption of those rules as the court or judge considers appropriate in the circumstances, shall apply to the appeal.

[2015 cA-1.2 s57](#)

[Back to Top](#)

Solicitor and client privilege

58. The solicitor and client privilege or litigation privilege of a record in dispute shall not be affected by disclosure to the Trial Division.

[2015 cA-1.2 s58](#)

[Back to Top](#)

Conduct of appeal

59. (1) The Trial Division shall review the decision, act or failure to act of the head of a public body that relates to a request for access to a record or correction of personal information under this Act as a new matter and may receive evidence by affidavit.

(2) The burden of proof in section 43 applies, with the necessary modifications, to an appeal.

(3) In exercising its powers to order production of documents for examination, the Trial Division shall take reasonable precautions, including where appropriate, receiving representations without notice to another person, conducting hearings in private and examining records in private, to avoid disclosure of

- (a) any information or other material if the nature of the information or material could justify a refusal by a head of a public body to give access to a record or part of a record;
or
- (b) the existence of information, where the head of a public body is authorized to refuse to confirm or deny that the information exists under subsection 17 (2).

[2015 cA-1.2 s59](#)

[Back to Top](#)

Disposition of appeal

60. (1) On hearing an appeal the Trial Division may

- (a) where it determines that the head of the public body is authorized to refuse access to a record under this Part and, where applicable, it has not been clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception, dismiss the appeal;
- (b) where it determines that the head of the public body is required to refuse access to a record under this Part, dismiss the appeal; or
- (c) where it determines that the head is not authorized or required to refuse access to all or part of a record under this Part,

- (i) order the head of the public body to give the applicant access to all or part of the record, and
- (ii) make an order that the court considers appropriate.

(2) Where the Trial Division finds that a record or part of a record falls within an exception to access under this Act and, where applicable, it has not been clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception, the court shall not order the head to give the applicant access to that record or part of it, regardless of whether the exception requires or merely authorizes the head to refuse access.

(3) Where the Trial Division finds that to do so would be in accordance with this Act or the regulations, it may order that personal information be corrected and the manner in which it is to be corrected.

[2015 cA-1.2 s60](#)

PART III PROTECTION OF PERSONAL INFORMATION

DIVISION 1 COLLECTION, USE AND DISCLOSURE

[Back to Top](#)

Purpose for which personal information may be collected

- 61.** No personal information may be collected by or for a public body unless
- (a) the collection of that information is expressly authorized by or under an Act;
 - (b) that information is collected for the purposes of law enforcement; or
 - (c) that information relates directly to and is necessary for an operating program or activity of the public body.

[2015 cA-1.2 s61](#)

[Back to Top](#)

How personal information is to be collected

62. (1) A public body shall collect personal information directly from the individual the information is about unless

- (a) another method of collection is authorized by
 - (i) that individual,
 - (ii) the commissioner under paragraph 95 (1)(c), or
 - (iii) an Act or regulation;
- (b) the information may be disclosed to the public body under sections 68 to 71 ;
- (c) the information is collected for the purpose of
 - (i) determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary,

- (ii) an existing or anticipated proceeding before a court or a judicial or quasi-judicial tribunal,
 - (iii) collecting a debt or fine or making a payment, or
 - (iv) law enforcement; or
- (d) collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual.
- (2) A public body shall tell an individual from whom it collects personal information
- (a) the purpose for collecting it;
 - (b) the legal authority for collecting it; and
 - (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.
- (3) Subsection (2) does not apply where
- (a) the information is about law enforcement or anything referred to in subsection 31 (1) or (2); or
 - (b) in the opinion of the head of the public body, complying with it would
 - (i) result in the collection of inaccurate information, or
 - (ii) defeat the purpose or prejudice the use for which the information is collected.

[2015 cA-1.2 s62](#)

[Back to Top](#)

Accuracy of personal information

63. Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete.

[2015 cA-1.2 s63](#)

[Back to Top](#)

Protection of personal information

64. (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that

- (a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;
- (b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and
- (c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

(2) For the purpose of paragraph (1)(c), "disposed of in a secure manner" in relation to the disposition of a record of personal information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.

(3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is

- (a) stolen;
- (b) lost;
- (c) disposed of, except as permitted by law; or
- (d) disclosed to or accessed by an unauthorized person.

(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.

(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by the head of a public body is not required, the commissioner may recommend that the head of the public body, at the first reasonable opportunity, notify the individual who is the subject of the information.

(6) Where a public body has received personal information from another public body for the purpose of research, the researcher may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the public body that provided the information to the researcher first obtains that individual's consent to contact by the researcher and informs the researcher that the individual has given consent.

(7) Subsection (3) does not apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information.

(8) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

(9) The factors that are relevant to determining under subsection (7) whether a breach creates a risk of significant harm to an individual include

- (a) the sensitivity of the personal information; and
- (b) the probability that the personal information has been, is being, or will be misused.

[2015 cA-1.2 s64](#)

[Back to Top](#)

Retention of personal information

65. (1) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

(2) A public body that has custody or control of personal information that is the subject of a request for access to a record or correction of personal information under Part II shall retain that information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request.

[2015 cA-1.2 s65](#)

[Back to Top](#)

Use of personal information

66. (1) A public body may use personal information only

- (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 69 ;
- (b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or
- (c) for a purpose for which that information may be disclosed to that public body under sections 68 to 71 .

(2) The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

[2015 cA-1.2 s66](#)

[Back to Top](#)

Use of personal information by post-secondary educational bodies

67. (1) Notwithstanding section 66 , a post-secondary educational body may, in accordance this section, use personal information in its alumni records for the purpose of its own fundraising activities where that personal information is reasonably necessary for the fundraising activities.

(2) In order to use personal information in its alumni records for the purpose of its own fundraising activities, a post-secondary educational body shall

- (a) give notice to the individual to whom the personal information relates when the individual is first contacted for the purpose of soliciting funds for fundraising of his or her right to request that the information cease to be used for fundraising purposes;
- (b) periodically and in the course of soliciting funds for fundraising, give notice to the individual to whom the personal information relates of his or her right to request that the information cease to be used for fundraising purposes; and
- (c) periodically and in a manner that is likely to come to the attention of individuals who may be solicited for fundraising, publish in an alumni magazine or other publication, a notice of the individual's right to request that the individual's personal information cease to be used for fundraising purposes.

(3) A post-secondary educational body shall, where requested to do so by an individual, cease to use the individual's personal information under subsection (1).

(4) The use of personal information by a post-secondary educational body under this section shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

[2015 cA-1.2 s67](#)

[Back to Top](#)

Disclosure of personal information

68. (1) A public body may disclose personal information only
- (a) in accordance with Part II;
 - (b) where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;
 - (c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 69 ;
 - (d) for the purpose of complying with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province or Canada ;
 - (e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information;
 - (f) to an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;
 - (g) to the Attorney General for use in civil proceedings involving the government;
 - (h) for the purpose of enforcing a legal right the government of the province or a public body has against a person;
 - (i) for the purpose of
 - (i) collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body, or
 - (ii) making a payment owing by the government of the province or by a public body to the individual the information is about;
 - (j) to the Auditor General or another person or body prescribed in the regulations for audit purposes;
 - (k) to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem;
 - (l) to a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;
 - (m) to the Provincial Archives of Newfoundland and Labrador , or the archives of a public body, for archival purposes;
 - (n) to a public body or a law enforcement agency in Canada to assist in an investigation
 - (i) undertaken with a view to a law enforcement proceeding, or
 - (ii) from which a law enforcement proceeding is likely to result;
 - (o) where the public body is a law enforcement agency and the information is disclosed
 - (i) to another law enforcement agency in Canada , or

- (ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;
 - (p) where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is given in the form appropriate in the circumstances to the individual the information is about;
 - (q) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted;
 - (r) in accordance with an Act of the province or Canada that authorizes or requires the disclosure;
 - (s) in accordance with sections 70 and 71 ;
 - (t) where the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 40 ;
 - (u) to an officer or employee of a public body or to a minister, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or minister to whom the information is disclosed; or
 - (v) to the surviving spouse or relative of a deceased individual where, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy.
- (2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.

[2015 cA-1.2 s68](#)

[Back to Top](#)

Definition of consistent purposes

69. A use of personal information is consistent under section 66 or 68 with the purposes for which the information was obtained or compiled where the use

- (a) has a reasonable and direct connection to that purpose; and
- (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

[2015 cA-1.2 s69](#)

[Back to Top](#)

Disclosure for research or statistical purposes

70. A public body may disclose personal information for a research purpose, including statistical research, only where

- (a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;
- (b) any record linkage is not harmful to the individuals that information is about and the benefits to be derived from the record linkage are clearly in the public interest;

- (c) the head of the public body concerned has approved conditions relating to the following:
 - (i) security and confidentiality,
 - (ii) the removal or destruction of individual identifiers at the earliest reasonable time, and
 - (iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public body; and
- (d) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and the public body's policies and procedures relating to the confidentiality of personal information.

[2015 cA-1.2 s70](#)

[Back to Top](#)

Disclosure for archival or historical purposes

71. The Provincial Archives of Newfoundland and Labrador , or the archives of a public body, may disclose personal information for archival or historical purposes where

- (a) the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 40 ;
- (b) the disclosure is for historical research and is in accordance with section 70 ;
- (c) the information is about an individual who has been dead for 20 years or more; or
- (d) the information is in a record that has been in existence for 50 years or more.

[2015 cA-1.2 s71](#)

[Back to Top](#)

Privacy impact assessment

72. (1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act

- (a) a privacy impact assessment for that minister's review and comment; or
- (b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.

(2) A minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.

(4) Where the minister responsible for this Act receives a privacy impact assessment respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68 (1)(u), the minister shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.

[2015 cA-1.2 s72](#)

**DIVISION 2
PRIVACY COMPLAINT**

[Back to Top](#)

Privacy complaint

73. (1) Where an individual believes on reasonable grounds that his or her personal information has been collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the commissioner.

(2) Where a person believes on reasonable grounds that personal information has been collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the commissioner on behalf of an individual or group of individuals, where that individual or those individuals have given consent to the filing of the privacy complaint.

(3) Where the commissioner believes that personal information has been collected, used or disclosed by a public body in contravention of this Act, the commissioner may on his or her own motion carry out an investigation.

(4) A privacy complaint under subsection (1) or (2) shall be filed in writing with the commissioner within

(a) one year after the subject matter of the privacy complaint first came to the attention of the complainant or should reasonably have come to the attention of the complainant; or

(b) a longer period of time as permitted by the commissioner.

(5) The commissioner shall provide a copy or summary of the privacy complaint, including an investigation initiated on the commissioner's own motion, to the head of the public body concerned.

[2015 cA-1.2 s73](#)

[Back to Top](#)

Investigation – privacy complaint

74. (1) The commissioner may take the steps that he or she considers appropriate to resolve a privacy complaint informally to the satisfaction of the parties and in a manner consistent with this Act.

(2) Where the commissioner is unable to informally resolve a privacy complaint within a reasonable period of time, the commissioner shall conduct a formal investigation of the subject matter of the privacy complaint where he or she is satisfied that there are reasonable grounds to do so.

(3) The commissioner shall complete a formal investigation and make a report under section 77 within a time that is as expeditious as possible in the circumstances.

(4) Where the commissioner has 5 active privacy complaints from the same person that deal with similar or related records, the commissioner may hold an additional complaint in abeyance and not commence an investigation until one of the 5 active complaints is resolved.

[2015 cA-1.2 s74](#)

[Back to Top](#)

Authority of commissioner not to investigate a privacy complaint

75. The commissioner may, at any stage of an investigation, refuse to investigate a privacy complaint where he or she is satisfied that

- (a) the head of a public body has responded adequately to the privacy complaint;
- (b) the privacy complaint has been or could be more appropriately dealt with by a procedure or proceeding other than a complaint under this Act;
- (c) the length of time that has elapsed between the date when the subject matter of the privacy complaint arose and the date when the privacy complaint was filed is such that an investigation under this Part would be likely to result in undue prejudice to a person or that a report would not serve a useful purpose; or
- (d) the privacy complaint is trivial, frivolous, vexatious or is made in bad faith.

[2015 cA-1.2 s75](#)

[Back to Top](#)

Recommendations – privacy complaint

76. (1) On completing an investigation of a privacy complaint, the commissioner may recommend that the head of a public body

- (a) stop collecting, using or disclosing personal information in contravention of this Act; or
 - (b) destroy personal information collected in contravention of this Act.
- (2) The commissioner may also make
- (a) a recommendation that an information practice, policy or procedure be implemented, modified, stopped or not commenced; or
 - (b) a recommendation on the privacy aspect of the matter that is the subject of the privacy complaint.

[2015 cA-1.2 s76](#)

[Back to Top](#)

Report – privacy complaint

77. (1) On completing an investigation of a privacy complaint, the commissioner shall

- (a) prepare a report containing the commissioner's findings and, where appropriate, his or her recommendations and the reasons for those recommendations; and
- (b) send a copy of the report to the person who filed the privacy complaint and the head of the public body concerned.

(2) The report shall include information respecting the obligation of the head of the public body to notify the person who filed the privacy complaint of the head's response to the recommendation of the commissioner within 10 business days of receipt of the recommendation.

[2015 cA-1.2 s77](#)

[Back to Top](#)

Response of public body – privacy complaint

78. (1) The head of a public body shall, not later than 10 business days after receiving a recommendation of the commissioner,

- (a) decide whether or not to comply with the recommendation in whole or in part; and
- (b) give written notice of his or her decision to the commissioner and a person who was sent a copy of the report.

(2) Where the head of the public body does not give written notice within the time required by subsection (1), the head of the public body is considered to have agreed to comply with the recommendation of the commissioner.

[2015 cA-1.2 s78](#)

[Back to Top](#)

Head of public body seeks declaration in court

79. (1) Where the head of the public body decides under section 78 not to comply with a recommendation of the commissioner under subsection 76 (1) in whole or in part, the head shall, not later than 10 business days after receipt of that recommendation,

- (a) apply to the Trial Division for a declaration that the public body is not required to comply with that recommendation because the collection, use or disclosure of the personal information is not in contravention of this Act, and
- (b) serve a copy of the application for a declaration on the commissioner, the minister responsible for the administration of this Act, and a person who was sent a copy of the commissioner's report.

(2) The commissioner or the minister responsible for this Act may intervene in an application for a declaration by filing a notice to that effect with the Trial Division.

[2015 cA-1.2 s79](#)

[Back to Top](#)

Filing an order with the Trial Division

80. (1) The commissioner may prepare and file an order with the Trial Division where

- (a) the head of the public body agrees or is considered to have agreed under section 78 to comply with a recommendation of the commissioner under subsection 76 (1) in whole or in part but fails to do so within one year after receipt of the commissioner's recommendation; or
- (b) the head of the public body fails to apply under section 79 to the Trial Division for a declaration.

(2) The order shall be limited to a direction to the head of the public body to do one or more of the following:

- (a) stop collecting, using or disclosing personal information in contravention of this Act; or
- (b) destroy personal information collected in contravention of this Act.

(3) An order shall not be filed with the Trial Division until the time period referred to in paragraph (1)(a) has passed.

(4) Where an order is filed with the Trial Division, it is enforceable against the public body as if it were a judgment or order made by the court.

[2015 cA-1.2 s80](#)

DIVISION 3 APPLICATION TO THE TRIAL DIVISION FOR A DECLARATION

[Back to Top](#)

Practice and procedure

81. The practice and procedure under the *Rules of the Supreme Court, 1986* providing for an expedited trial, or such adaptation of those rules as the court or judge considers appropriate in the circumstances, shall apply to an application to the Trial Division for a declaration.

[2015 cA-1.2 s81](#)

[Back to Top](#)

Solicitor and client privilege

82. The solicitor and client privilege or litigation privilege of a record which may contain personal information shall not be affected by disclosure to the Trial Division.

[2015 cA-1.2 s82](#)

[Back to Top](#)

Conduct

83. (1) The Trial Division shall review the act or failure to act of the head of a public body that relates to the collection, use or disclosure of personal information under this Act as a new matter and may receive evidence by affidavit.

(2) In exercising its powers to order production of documents for examination, the Trial Division shall take reasonable precautions, including where appropriate, receiving representations without notice to another person, conducting hearings in private and examining records in private, to avoid disclosure of

(a) any information or other material if the nature of the information or material could justify a refusal by a head of a public body to give access to a record or part of a record;
or

(b) the existence of information, where the head of a public body is authorized to refuse to confirm or deny that the information exists under subsection 17 (2).

[2015 cA-1.2 s83](#)

[Back to Top](#)

Disposition

84. On hearing an application for a declaration, the Trial Division may

(a) where it determines that the head of the public body is authorized under this Act to use, collect or disclose the personal information, dismiss the application;

- (b) where it determines that the head is not authorized under this Act to use, collect or disclose the personal information,
 - (i) order the head of the public body to stop using, collecting or disclosing the information, or
 - (ii) order the head of the public body to destroy the personal information that was collected in contravention of this Act; or
- (c) make an order that the court considers appropriate.

[2015 cA-1.2 s84](#)

**PART IV
OFFICE AND POWERS OF THE INFORMATION AND PRIVACY
COMMISSIONER**

**DIVISION 1
OFFICE**

[Back to Top](#)

Appointment of the Information and Privacy Commissioner

- 85.** (1) The office of the Information and Privacy Commissioner is continued.
- (2) The office shall be filled by the Lieutenant-Governor in Council on a resolution of the House of Assembly.
- (3) Before an appointment is made, the Speaker shall establish a selection committee comprising
- (a) the Clerk of the Executive Council or his or her deputy;
 - (b) the Clerk of the House of Assembly or, where the Clerk is unavailable, the Clerk Assistant of the House of Assembly;
 - (c) the Chief Judge of the Provincial Court or another judge of that court designated by the Chief Judge; and
 - (d) the President of Memorial University or a vice-president of Memorial University designated by the President.
- (4) The selection committee shall develop a roster of qualified candidates and in doing so may publicly invite expressions of interest for the position of commissioner.
- (5) The selection committee shall submit the roster to the Speaker of the House of Assembly.
- (6) The Speaker shall
- (a) consult with the Premier, the Leader of the Official Opposition and the leader or member of a registered political party that is represented on the House of Assembly Management Commission; and
 - (b) cause to be placed before the House of Assembly a resolution to appoint as commissioner one of the individuals named on the roster.

[2015 cA-1.2 s85](#)

[Back to Top](#)

Status of the commissioner

86. (1) The commissioner is an officer of the House of Assembly and is not eligible to be nominated for election, to be elected, or to sit as a member of the House of Assembly.

(2) The commissioner shall not hold another public office or carry on a trade, business or profession.

(3) In respect of his or her interactions with a public body, whether or not it is a public body to which this Act applies, the commissioner has the status of a deputy minister.

[2015 cA-1.2 s86](#)

[Back to Top](#)

Term of office

87. (1) Unless he or she sooner resigns, dies or is removed from office, the commissioner shall hold office for 6 years from the date of his or her appointment.

(2) The Lieutenant-Governor in Council may, with the approval of a majority of the members on the government side of the House of Assembly and separate approval of a majority of the members on the opposition side of the House of Assembly, re-appoint the commissioner for one further term of 6 years.

(3) The Speaker shall, in the event of a tie vote on either or both sides of the House of Assembly, cast the deciding vote.

(4) The commissioner may resign his or her office in writing addressed to the Speaker of the House of Assembly, or, where there is no Speaker or the Speaker is absent, to the Clerk of the House of Assembly.

[2015 cA-1.2 s87](#)

[Back to Top](#)

Removal or suspension

88. (1) The Lieutenant-Governor in Council, on a resolution of the House of Assembly passed by a majority vote of the members of the House of Assembly actually voting, may remove the commissioner from office or suspend him or her because of an incapacity to act, or for neglect of duty or for misconduct.

(2) When the House of Assembly is not in session, the Lieutenant-Governor in Council may suspend the commissioner because of an incapacity to act, or for neglect of duty or for misconduct, but the suspension shall not continue in force beyond the end of the next sitting of the House of Assembly.

[2015 cA-1.2 s88](#)

[Back to Top](#)

Acting commissioner

89. (1) The Lieutenant-Governor in Council may, on the recommendation of the House of Assembly Management Commission, appoint an acting commissioner if

- (a) the commissioner is temporarily unable to perform his or her duties;
- (b) the office of the commissioner becomes vacant or the commissioner is suspended when the House of Assembly is not in session; or
- (c) the office of the commissioner becomes vacant or the commissioner is suspended when the House of Assembly is in session, but the House of Assembly does not pass a resolution to fill the office of the commissioner before the end of the session.

(2) Where the office of the commissioner becomes vacant and an acting commissioner is appointed under paragraph (1)(b) or (c), the term of the acting commissioner shall not extend beyond the end of the next sitting of the House of Assembly.

(3) An acting commissioner holds office until

- (a) the commissioner returns to his or her duties after a temporary inability to perform;
- (b) the suspension of the commissioner ends or is dealt with in the House of Assembly; or
- (c) a person is appointed as a commissioner under section 85 .

[2015 cA-1.2 s89](#)

[Back to Top](#)

Salary, pension and benefits

90. (1) The commissioner shall be paid a salary fixed by the Lieutenant-Governor in Council after consultation with the House of Assembly Management Commission.

(2) The salary of the commissioner shall not be reduced except on resolution of the House of Assembly.

(3) The commissioner is subject to the *Public Service Pensions Act, 1991* where he or she was subject to that Act prior to his or her appointment as commissioner.

(4) Where the commissioner is not subject to the *Public Service Pensions Act, 1991* prior to his or her appointment as commissioner, he or she shall be paid, for contribution to a registered retirement savings plan, an amount equivalent to the amount which he or she would have contributed to the Public Service Pension Plan were the circumstances in subsection (3) applicable.

(5) The commissioner is eligible to receive the same benefits as a deputy minister, with the exception of a pension where subsection (4) applies.

[2015 cA-1.2 s90; 2016 c6 s2](#)

[Back to Top](#)

Expenses

91. The commissioner shall be paid the travelling and other expenses, at the deputy minister level, incurred by him or her in the performance of his or her duties that may be approved by the House of Assembly Management Commission.

[2015 cA-1.2 s91](#)

[Back to Top](#)

Commissioner's staff

92. (1) The commissioner may, subject to the approval of the House of Assembly Management Commission, and in the manner provided by law, appoint those assistants and employees that he or she considers necessary to enable him or her to carry out his or her functions under this Act and the *Personal Health Information Act* .

(2) Persons employed under subsection (1) are members of the public service of the province.

[2015 cA-1.2 s92](#)

[Back to Top](#)

Oath of office

93. Before beginning to perform his or her duties, the commissioner shall swear an oath, or affirm, before the Speaker of the House of Assembly or the Clerk of the House of Assembly that he or she shall faithfully and impartially perform the duties of his or her office and that he or she shall not, except as provided by this Act and the *Personal Health Information Act* , divulge information received by him or her under this Act and the *Personal Health Information Act* .

[2015 cA-1.2 s93](#)

[Back to Top](#)

Oath of staff

94. Every person employed under the commissioner shall, before he or she begins to perform his or her duties, swear an oath, or affirm, before the commissioner that he or she shall not, except as provided by this Act and the *Personal Health Information Act* , divulge information received by him or her under this Act and the *Personal Health Information Act* .

[2015 cA-1.2 s94](#)

DIVISION 2 POWERS OF THE COMMISSIONER

[Back to Top](#)

General powers and duties of commissioner

95. (1) In addition to the commissioner's powers and duties under Parts II and III, the commissioner may

- (a) conduct investigations to ensure compliance with this Act and the regulations;
- (b) monitor and audit the practices and procedures employed by public bodies in carrying out their responsibilities and duties under this Act;
- (c) review and authorize the collection of personal information from sources other than the individual the information is about;
- (d) consult with any person with experience or expertise in any matter related to the purpose of this Act; and
- (e) engage in or commission research into anything relating to the purpose of this Act.

(2) In addition to the commissioner's powers and duties under Parts II and III, the commissioner shall exercise and perform the following powers and duties:

- (a) inform the public about this Act;
- (b) develop and deliver an educational program to inform people of their rights and the reasonable limits on those rights under this Act and to inform public bodies of their responsibilities and duties, including the duty to assist, under this Act;
- (c) provide reasonable assistance, upon request, to a person;
- (d) receive comments from the public about the administration of this Act and about matters concerning access to information and the confidentiality, protection and correction of personal information;
- (e) comment on the implications for access to information or for protection of privacy of proposed legislative schemes, programs or practices of public bodies;
- (f) comment on the implications for protection of privacy of
 - (i) using or disclosing personal information for record linkage, or
 - (ii) using information technology in the collection, storage, use or transfer of personal information;
- (g) take actions necessary to identify, promote, and where possible cause to be made adjustments to practices and procedures that will improve public access to information and protection of personal information;
- (h) bring to the attention of the head of a public body a failure to fulfil the duty to assist applicants;
- (i) make recommendations to the head of a public body or the minister responsible for this Act about the administration of this Act;
- (j) inform the public from time to time of apparent deficiencies in the system, including the office of the commissioner; and
- (k) establish and implement practices and procedures in the office of the commissioner to ensure efficient and timely compliance with this Act.

(3) The commissioner's investigation powers and duties provided in this Part are not limited to an investigation under paragraph (1)(a) but apply also to an investigation in respect of a complaint, privacy complaint, audit, decision or other action that the commissioner is authorized to take under this Act.

[2015 cA-1.2 s95](#)

[Back to Top](#)

Representation during an investigation

96. (1) During an investigation, the commissioner may give a person an opportunity to make a representation.

(2) An investigation may be conducted by the commissioner in private and a person who makes representations during an investigation is not, except to the extent invited by the commissioner to do so, entitled to be present during an investigation or to comment on representations made to the commissioner by another person.

(3) The commissioner may decide whether representations are to be made orally or in writing.

(4) Representations may be made to the commissioner through counsel or an agent.

[2015 cA-1.2 s96](#)

[Back to Top](#)

Production of documents

97. (1) This section and section 98 apply to a record notwithstanding

(a) paragraph 5 (1)(c), (d), (e), (f), (g), (h) or (i);

(b) subsection 7 (2);

(c) another Act or regulation; or

(d) a privilege under the law of evidence.

(2) The commissioner has the powers, privileges and immunities that are or may be conferred on a commissioner under the *Public Inquiries Act, 2006* .

(3) The commissioner may require any record in the custody or under the control of a public body that the commissioner considers relevant to an investigation to be produced to the commissioner and may examine information in a record, including personal information.

(4) As soon as possible and in any event not later than 10 business days after a request is made by the commissioner, the head of a public body shall produce to the commissioner a record or a copy of a record required under this section.

(5) The head of a public body may require the commissioner to examine the original record at a site determined by the head where

(a) the head of the public body has a reasonable basis for concern about the security of a record that is subject to solicitor and client privilege or litigation privilege;

(b) the head of the public body has a reasonable basis for concern about the security of another record and the Commissioner agrees there is a reasonable basis for concern; or

(c) it is not practicable to make a copy of the record.

(6) The head of a public body shall not place a condition on the ability of the commissioner to access or examine a record required under this section, other than that provided in subsection (5).

[2015 cA-1.2 s97](#)

[Back to Top](#)

Right of entry

98. The commissioner has the right

(a) to enter an office of a public body and examine and make copies of a record in the custody of the public body; and

(b) to converse in private with an officer or employee of the public body.

[2015 cA-1.2 s98](#)

[Back to Top](#)

Admissibility of evidence

99. (1) A statement made, or answer or evidence given by a person in the course of an investigation by or proceeding before the commissioner under this Act is not admissible in evidence against a person in a court or at an inquiry or in another proceeding, and no evidence respecting a proceeding under this Act shall be given against a person except

- (a) in a prosecution for perjury;
- (b) in a prosecution for an offence under this Act; or
- (c) in an appeal to, or an application for a declaration from, the Trial Division under this Act, or in an appeal to the Court of Appeal respecting a matter under this Act.

(2) The commissioner, and a person acting for or under the direction of the commissioner, shall not be required to give evidence in a court or in a proceeding about information that comes to the knowledge of the commissioner in performing duties or exercising powers under this Act.

[2015 cA-1.2 s99](#)

[Back to Top](#)

Privilege

100. (1) Where a person speaks to, supplies information to or produces a record during an investigation by the commissioner under this Act, what he or she says, the information supplied and the record produced are privileged in the same manner as if they were said, supplied or produced in a proceeding in a court.

(2) The solicitor and client privilege or litigation privilege of the records shall not be affected by production to the commissioner.

[2015 cA-1.2 s100](#)

[Back to Top](#)

Section 8.1 of the *Evidence Act*

101. Section 8.1 of the *Evidence Act* does not apply to an investigation conducted by the commissioner under this Act.

[2015 cA-1.2 s101](#)

[Back to Top](#)

Disclosure of information

102. (1) The commissioner and a person acting for or under the direction of the commissioner, shall not disclose information obtained in performing duties or exercising powers under this Act, except as provided in subsections (2) to (5).

(2) The commissioner may disclose, or may authorize a person acting for or under his or her direction to disclose, information that is necessary to

- (a) perform a duty or exercise a power of the commissioner under this Act; or

(b) establish the grounds for findings and recommendations contained in a report under this Act.

(3) In conducting an investigation and in performing a duty or exercising a power under this Act, the commissioner and a person acting for or under his or her direction, shall take reasonable precautions to avoid disclosing and shall not disclose

(a) any information or other material if the nature of the information or material could justify a refusal by a head of a public body to give access to a record or part of a record;

(b) the existence of information, where the head of a public body is authorized to refuse to confirm or deny that the information exists under subsection 17 (2);

(c) any information contained in a report or notice made under section 4 or 7 of the *Patient Safety Act* ; or

(d) any information, including a record, that is prepared for the use of, or collected, compiled or prepared by, a committee referred to in subsection 8.1(1) of the *Evidence Act* for the purpose of carrying out its duties.

(4) The commissioner may disclose to the Attorney General information relating to the commission of an offence under this or another Act of the province or Canada , where the commissioner has reason to believe an offence has been committed.

(5) The commissioner may disclose, or may authorize a person acting for or under his or her direction to disclose, information in the course of a prosecution or another matter before a court referred to in subsection 99 (1).

[2015 cA-1.2 s102; 2017 cP-3.01 s28](#)

[Back to Top](#)

Delegation

103. The commissioner may delegate to a person on his or her staff a duty or power under this Act.

[2015 cA-1.2 s103](#)

[Back to Top](#)

Protection from liability

104. An action does not lie against the commissioner or against a person employed under him or her for anything he or she may do or report or say in the course of the exercise or performance, or intended exercise or performance, of his or her functions and duties under this Act, unless it is shown he or she acted in bad faith.

[2015 cA-1.2 s104](#)

[Back to Top](#)

Annual report

105. The commissioner shall report annually to the House of Assembly through the Speaker on

(a) the exercise and performance of his or her duties and functions under this Act;

(b) a time analysis of the functions and procedures in matters involving the commissioner in a complaint, from the date of receipt of the request for access or correction by the public

body to the date of informal resolution, the issuing of the commissioner's report, or the withdrawal or abandonment of the complaint, as applicable;

- (c) persistent failures of public bodies to fulfil the duty to assist applicants, including persistent failures to respond to requests in a timely manner;
- (d) the commissioner's recommendations and whether public bodies have complied with the recommendations;
- (e) the administration of this Act by public bodies and the minister responsible for this Act; and
- (f) other matters about access to information and protection of privacy that the commissioner considers appropriate.

[2015 cA-1.2 s105](#)

[Back to Top](#)

Special report

106. The commissioner may at any time make a special report to the House of Assembly through the Speaker relating to

- (a) the resources of the office of the commissioner;
- (b) another matter affecting the operations of this Act; or
- (c) a matter within the scope of the powers and duties of the commissioner under this Act.

[2015 cA-1.2 s106](#)

[Back to Top](#)

Report – investigation or audit

107. On completing an investigation under paragraph 95 (1)(a) or an audit under paragraph 95 (1)(b), the commissioner

- (a) shall prepare a report containing the commissioner's findings and, where appropriate, his or her recommendations and the reasons for those recommendations;
- (b) shall send a copy of the report to the head of the public body concerned; and
- (c) may make the report public.

[2015 cA-1.2 s107](#)

PART V GENERAL

[Back to Top](#)

Exercising rights of another person

108. A right or power of an individual given in this Act may be exercised

- (a) by a person with written authorization from the individual to act on the individual's behalf;

- (b) by a court appointed guardian of a mentally disabled person, where the exercise of the right or power relates to the powers and duties of the guardian;
- (c) by an attorney acting under a power of attorney, where the exercise of the right or power relates to the powers and duties conferred by the power of attorney;
- (d) by the parent or guardian of a minor where, in the opinion of the head of the public body concerned, the exercise of the right or power by the parent or guardian would not constitute an unreasonable invasion of the minor's privacy; or
- (e) where the individual is deceased, by the individual's personal representative, where the exercise of the right or power relates to the administration of the individual's estate.

[2015 cA-1.2 s108](#)

[Back to Top](#)

Designation of head by local public body

109. (1) A local public body shall, by by-law, resolution or other instrument, designate a person or group of persons as the head of the local public body for the purpose of this Act, and once designated, the local public body shall advise the minister responsible for this Act of the designation.

- (2) A local government body or group of local government bodies shall
 - (a) by by-law, resolution or other instrument, designate a person or group of persons, for the purpose of this Act, as the head of an unincorporated entity owned by or created for the local government body or group of local government bodies; and
 - (b) advise the minister responsible for this Act of the designation.

[2015 cA-1.2 s109](#)

[Back to Top](#)

Designation and delegation by the head of a public body

110. (1) The head of a public body shall designate a person on the staff of the public body as the coordinator to

- (a) receive and process requests made under this Act;
- (b) co-ordinate responses to requests for approval by the head of the public body;
- (c) communicate, on behalf of the public body, with applicants and third parties to requests throughout the process including the final response;
- (d) educate staff of the public body about the applicable provisions of this Act;
- (e) track requests made under this Act and the outcome of the request;
- (f) prepare statistical reports on requests for the head of the public body; and
- (g) carry out other duties as may be assigned.

(2) The head of a public body may delegate to a person on the staff of the public body a duty or power of the head under this Act.

[2015 cA-1.2 s110](#)

[Back to Top](#)

Publication scheme

111. (1) The commissioner shall create a standard template for the publication of information by public bodies to assist in identifying and locating records in the custody or under the control of public bodies.

(2) The head of a public body shall adapt the standard template to its functions and publish its own information according to that adapted template.

(3) The published information shall include

(a) a description of the mandate and functions of the public body and its components;

(b) a description and list of the records in the custody or under the control of the public body, including personal information banks;

(c) the name, title, business address and business telephone number of the head and coordinator of the public body; and

(d) a description of the manuals used by employees of the public body in administering or carrying out the programs and activities of the public body.

(4) The published information shall include for each personal information bank maintained by a public body

(a) its name and location;

(b) a description of the kind of personal information and the categories of individuals whose personal information is included;

(c) the authority and purposes for collecting the personal information;

(d) the purposes for which the personal information is used or disclosed; and

(e) the categories of persons who use the personal information or to whom it is disclosed.

(5) Where personal information is used or disclosed by a public body for a purpose that is not included in the information published under subsection (2), the head of the public body shall

(a) keep a record of the purpose and either attach or link the record to the personal information; and

(b) update the published information to include that purpose.

(6) This section or a subsection of this section shall apply to those public bodies listed in the regulations.

[2015 cA-1.2 s111](#)

[Back to Top](#)

Amendments to statutes and regulations

112. (1) A minister shall consult with the commissioner on a proposed Bill that could have implications for access to information or protection of privacy, as soon as possible before, and not later than, the date on which notice to introduce the Bill in the House of Assembly is given.

(2) The commissioner shall advise the minister as to whether the proposed Bill has implications for access to information or protection of privacy.

(3) The commissioner may comment publicly on a draft Bill any time after that draft Bill has been made public.

[2015 cA-1.2 s112](#)

[Back to Top](#)

Report of minister responsible

113. The minister responsible for this Act shall report annually to the House of Assembly on the administration of this Act and shall include information about

- (a) the number of requests for access and whether they were granted or denied;
- (b) the specific provisions of this Act used to refuse access;
- (c) the number of requests for correction of personal information;
- (d) the costs charged for access to records; and
- (e) systemic and other issues raised by the commissioner in the annual reports of the commissioner.

[2015 cA-1.2 s113](#)

[Back to Top](#)

Limitation of liability

114. (1) An action does not lie against the government of the province, a public body, the head of a public body, an elected or appointed official of a local public body or a person acting for or under the direction of the head of a public body for damages resulting from

- (a) the disclosure of or a failure to disclose, in good faith, a record or part of a record or information under this Act or a consequence of that disclosure or failure to disclose; or
- (b) the failure to give a notice required by this Act where reasonable care is taken to ensure that notices are given.

(2) An action does not lie against a Member of the House of Assembly for disclosing information obtained from a public body in accordance with paragraph 68 (1)(k) while acting in good faith on behalf of an individual.

[2015 cA-1.2 s114](#)

[Back to Top](#)

Offence

115. (1) A person who wilfully collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence and liable, on summary conviction, to a fine of not more than \$10,000 or to imprisonment for a term not exceeding 6 months, or to both.

- (2) A person who wilfully

- (a) attempts to gain or gains access to personal information in contravention of this Act or the regulations;
- (b) makes a false statement to, or misleads or attempts to mislead the commissioner or another person performing duties or exercising powers under this Act;
- (c) obstructs the commissioner or another person performing duties or exercising powers under this Act;
- (d) destroys a record or erases information in a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records; or
- (e) alters, falsifies or conceals a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records,

is guilty of an offence and liable, on summary conviction, to a fine of not more than \$10,000 or to imprisonment for a term not exceeding 6 months, or to both.

(3) A prosecution for an offence under this Act shall be commenced within 2 years of the date of the discovery of the offence.

[2015 cA-1.2 s115](#)

[Back to Top](#)

Regulations

116. The Lieutenant-Governor in Council may make regulations

- (a) designating a body as a public body, educational body, health care body or local government body under this Act;
- (b) designating a person or group of persons as the head of a public body;
- (c) prescribing procedures to be followed in making, transferring and responding to requests under this Act;
- (d) permitting prescribed categories of applicants to make requests under this Act orally instead of in writing;
- (e) limiting the costs that different categories of persons may be charged under this Act;
- (f) authorizing, for the purposes of section 28 , a local public body to hold meetings of its elected officials, or of its governing body or a committee of the governing body, to consider specified matters in the absence of the public unless another Act
 - (i) expressly authorizes the local public body to hold meetings in the absence of the public, and
 - (ii) specifies the matters that may be discussed at those meetings;
- (g) prescribing for the purposes of section 36 the categories of sites that are considered to have heritage or anthropological value;
- (h) authorizing the disclosure of information relating to the mental or physical health of individuals to medical or other experts to determine, for the purposes of section 37 , if disclosure of that information could reasonably be expected to result in grave and immediate harm to the safety of or the mental or physical health of those individuals;

- (i) prescribing procedures to be followed or restrictions considered necessary with respect to the disclosure and examination of information referred to in paragraph (h);
- (j) prescribing special procedures for giving individuals access to personal information about their mental or physical health;
- (k) prescribing, for the purposes of section 68 , a body to whom personal information may be disclosed for audit purposes;
- (l) prescribing the public bodies that are required to comply with all or part of section 111 ;
- (m) requiring public bodies to provide to the minister responsible for this Act information that relates to its administration or is required for preparing the minister's annual report;
- (n) providing for the retention and disposal of records by a public body if the *Management of Information Act* does not apply to the public body;
- (o) exempting any class of public body from a regulation made under this section; and
- (p) generally to give effect to this Act.

[2015 cA-1.2 s116](#)

[Back to Top](#)

Review

117. (1) After the expiration of not more than 5 years after the coming into force of this Act or part of it and every 5 years thereafter, the minister responsible for this Act shall refer it to a committee for the purpose of undertaking a comprehensive review of the provisions and operation of this Act or part of it.

(2) The committee shall review the list of provisions in Schedule A to determine the necessity for their continued inclusion in Schedule A.

[2015 cA-1.2 s117](#)

[Back to Top](#)

Transitional

118. (1) This Act applies to

- (a) a request for access to a record that is made on or after the day section 8 comes into force;
 - (b) a request for correction of personal information that is made on or after the day section 10 comes into force; and
 - (c) a privacy complaint that is filed by an individual or commenced by the commissioner on or after the day section 73 comes into force.
- (2) Part IV, Division 1 applies to and upon the appointment of the next commissioner.

[2015 cA-1.2 s118](#)

[Back to Top](#)

SNL2013 cA-3.1 Amdt.

119. (1) Subsection 61(2) of the *Adoption Act, 2013* is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

(2) Section 64 of the Act is repealed and the following substituted:

[Back to Top](#)

Acts do not apply

64. Notwithstanding the *Access to Information and Protection of Privacy Act, 2015* and the *Privacy Act* (Canada), the use of, disclosure of and access to information in records pertaining to adoptions, regardless of where the information or records are located, shall be governed by this Act.

(3) Subsection 67(1) of the Act is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s119](#)

[Back to Top](#)

SNL1991 c22 Amdt.

120. Section 19 of the *Auditor General Act* is repealed and the following substituted:

[Back to Top](#)

Prohibition

19. Notwithstanding sections 17 and 18, the auditor general shall not be permitted access to information the disclosure of which may be refused under section 31 of the *Access to Information and Protection of Privacy Act, 2015* or the disclosure of which shall be refused under section 27 of that Act.

[2015 cA-1.2 s120](#)

[Back to Top](#)

RSNL1990 cC-2 Amdt.

121. Subsection 201.83(2) of the *Canada-Newfoundland And Labrador Atlantic Accord Implementation Newfoundland And Labrador Act* is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s121](#)

[Back to Top](#)

SNL2004 cC-5.1 Amdt.

122. Paragraph 2(e) of the *Centre for Health Information Act* is repealed and the following substituted:

(e) "personal information" means personal information as defined in the *Access to Information and Protection of Privacy Act, 2015* , other than information described in subparagraph 2(u)(vi) of that Act.

[2015 cA-1.2 s122](#)

[Back to Top](#)

SNL2010 cC-12.2 Amdt.

123. (1) Section 69 of the *Children and Youth Care and Protection Act* is repealed and the following substituted:

[Back to Top](#)

Access to Information and Protection of Privacy Act, 2015 does not apply

69. Notwithstanding the *Access to Information and Protection of Privacy Act, 2015*, the use of, disclosure of and access to information in records pertaining to the care and protection of children and youth obtained under this Act, regardless of where the information or records are located, shall be governed by this Act.

(2) Subsection 74(1) of the Act is amended by deleting the reference "*Access to Information and Protection of Privacy Act*" and substituting the reference "*Access to Information and Protection of Privacy Act, 2015*".

[2015 cA-1.2 s123](#)

[Back to Top](#)

SNL2001 cC-14.1 Amdt.

124. Paragraph 19(e) of the *Citizens' Representative Act* is amended by deleting the reference "*Access to Information and Protection of Privacy Act*" and substituting the reference "*Access to Information and Protection of Privacy Act, 2015*".

[2015 cA-1.2 s124](#)

[Back to Top](#)

SNL2007 cE-11.01 Amdt.

125. (1) Paragraphs 2(h.1) and (h.2) of the *Energy Corporation Act* are amended by deleting the reference "*Access to Information and Protection of Privacy Act*" wherever it occurs and substituting the reference "*Access to Information and Protection of Privacy Act, 2015*".

(2) Subsections 5.4(1) to (4) are repealed and the following substituted:

[Back to Top](#)

Records of commercially sensitive information

5.4 (1) Notwithstanding section 7 of the *Access to Information and Protection of Privacy Act, 2015*, in addition to the information that shall or may be refused under Part II, Division 2 of that Act, the chief executive officer of the corporation or a subsidiary, or the head of another public body,

- (a) may refuse to disclose to an applicant under that Act commercially sensitive information of the corporation or the subsidiary; and
- (b) shall refuse to disclose to an applicant under that Act commercially sensitive information of a third party

where the chief executive officer of the corporation or the subsidiary to which the requested information relates, taking into account sound and fair business practices, reasonably believes

- (c) that the disclosure of the information may

- (i) harm the competitive position of,
 - (ii) interfere with the negotiating position of, or
 - (iii) result in financial loss or harm to
- the corporation, the subsidiary or the third party; or
- (d) that information similar to the information requested to be disclosed
 - (i) is treated consistently in a confidential manner by the third party, or
 - (ii) is customarily not provided to competitors by the corporation, the subsidiary or the third party.

(2) Where an applicant is denied access to information under subsection (1) and a request to review that decision is made to the commissioner under section 42 of the *Access to Information and Protection of Privacy Act, 2015*, the commissioner shall, where he or she determines that the information is commercially sensitive information,

- (a) on receipt of the chief executive officer's certification that he or she has refused to disclose the information for the reasons set out in subsection (1); and
- (b) confirmation of the chief executive officer's decision by the board of directors of the corporation or subsidiary,

uphold the decision of the chief executive officer or head of another public body not to disclose the information.

- (3) Where a person appeals,
 - (a) under subsections 52 (1) and (2), subsections 53 (1) and (2) or section 54 of the *Access to Information and Protection of Privacy Act, 2015*, from a decision under subsection (1); or
 - (b) under subsections 52 (1) and (2), subsections 53 (1) and (2) or section 54 of the *Access to Information and Protection of Privacy Act, 2015*, from a refusal by a chief executive officer under subsection (1) to disclose information,

paragraph 59 (3)(a) and section 60 of that Act apply to that appeal as if Part II, Division 2 included the grounds for the refusal to disclose the information set out in subsection (1) of this Act.

(4) Paragraph 102 (3)(a) of the *Access to Information and Protection of Privacy Act, 2015* applies to information referred to in subsection (1) of this section as if the information was information that a head of a public body is authorized or required to refuse to disclose under Part II, Division 2.

[2015 cA-1.2 s125](#)

[Back to Top](#)

SNL1995 cP-37.1 Amdt.

126. Section 4.01 of the *Health and Community Services Act* is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s126](#)

[Back to Top](#)

RSNL1990 cH-10 Amdt.

127. Section 50 of the *House of Assembly Act* is repealed and the following substituted:

[Back to Top](#)

Information exempt

50. Information disclosed by a member or the member's family to the commissioner under this Part or a regulation made under this Part or in the course of the administration of this Part shall not be disclosed under the *Access to Information and Protection of Privacy Act, 2015* or otherwise than in accordance with this Part.

[2015 cA-1.2 s127](#)

[Back to Top](#)

SNL2007cH-10.1 Amdt.

128. (1) Paragraph 32(2)(c) of the *House of Assembly Accountability, Integrity and Administration Act* is repealed and the following substituted:

(c) subsection 92(1) of the *Access to Information and Protection of Privacy Act, 2015* ;

(2) Subsection 49(1) of the Act is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s128](#)

[Back to Top](#)

SNL1999 cM-5.1 Amdt.

129. Paragraph 3(1)(e.1) of the *Medical Care Insurance Act, 1999* is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s129](#)

[Back to Top](#)

SNL2014 cM-16.2 Amdt.

130. Paragraph 2(g) of the *Missing Persons Act* is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s130](#)

[Back to Top](#)

SNL2008 cP-7.01 Amdt.

131. (1) Paragraphs 2(1)(e) and (r) of the *Personal Health Information Act* are amended by deleting the reference "*Access to Information and Protection of Privacy Act* " wherever it occurs and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

(2) Section 12 of the Act is repealed and the following substituted:

[Back to Top](#)

Access to information legislation

12. (1) The *Access to Information and Protection of Privacy Act, 2015* does not apply to

- (a) the use, collection, disclosure, storage, disposition or any other dealing with personal health information by or in the custody or control of a custodian;
- (b) a request for access to or correction of a record of personal health information in the custody or control of a custodian;
- (c) a complaint to the commissioner respecting
 - (i) a denial of access to or correction of a record of personal health information by a custodian,
 - (ii) a request for review or appeal of a denial of access to or correction of a record of personal health information by a custodian, or
 - (iii) a contravention or alleged contravention of this Act or the regulations; or
- (d) the determination or prosecution of an offence or the imposition of a penalty in respect of a breach of this Act or the regulations.

(2) Notwithstanding subsection (1), this Act does not limit a person's right of access under section 8 of the *Access to Information and Protection of Privacy Act, 2015*

- (a) to personal information contained in a record, other than a record referred to in subsection 5(4), in the custody or control of a custodian who is a public body, that contains both personal health information as described in section 5 and personal information but only where the personal information can be reasonably severed from the record;
- (b) to a record of personal health information which is in the custody or control of a public body who is not a custodian within the meaning of subsection 4(1); or
- (c) to both personal health information and personal information contained in a record referred to in subsection 5(4) where the record is in the custody or control of a custodian that is a public body.

(3) For the purpose of subsection (2), "personal information" means personal information as defined in paragraph 2 (u) of the *Access to Information and Protection of Privacy Act, 2015*, other than information referred to in subparagraph 2 (u)(vi) of that Act.

[2015 cA-1.2 s131](#)

[Back to Top](#)

SNL2008 cR-13.1 Amdt.

132. Subsections 21(1) to (4) of the *Research and Development Council Act* are repealed and the following substituted:

[Back to Top](#)

Records of commercially sensitive information

21. (1) Notwithstanding section 7 of the *Access to Information and Protection of Privacy Act, 2015*, in addition to the information that shall or may be refused under Part II, Division 2 of that Act, the chief executive officer, or the head of another public body,

- (a) may refuse to disclose to an applicant under that Act commercially sensitive information of the council; and
- (b) shall refuse to disclose to an applicant under that Act commercially sensitive information of a third party

where the chief executive officer, taking into account sound and fair business practices, reasonably believes

- (c) that the disclosure of the information may
 - (i) harm the competitive position of,
 - (ii) interfere with the negotiating position of, or
 - (iii) result in financial loss or harm to the council or the third party; or
- (d) that information similar to the information requested to be disclosed
 - (i) is treated consistently in a confidential manner by the third party, or
 - (ii) is customarily not provided to competitors by the council or the third party.

(2) Where an applicant is denied access to information under subsection (1) and a request to review that decision is made to the commissioner under section 42 of the *Access to Information and Protection of Privacy Act, 2015*, the commissioner shall, where he or she determines that the information is commercially sensitive information,

- (a) on receipt of the chief executive officer's certification that he or she has refused to disclose the information for the reasons set out in subsection (1); and
- (b) on confirmation of the chief executive officer's decision by the board of directors of the council,

uphold the decision of the chief executive officer or head of another public body not to disclose the information.

- (3) Where a person appeals,
 - (a) under subsections 52 (1) and (2), subsections 53 (1) and (2) or section 54 of the *Access to Information and Protection of Privacy Act, 2015*, from a decision under subsection (1); or
 - (b) under subsections 52 (1) and (2), subsections 53 (1) and (2) or section 54 of the *Access to Information and Protection of Privacy Act, 2015*, from a refusal by a chief executive officer under subsection (1) to disclose information,

paragraph 59 (3)(a) and section 60 of that Act apply to that appeal as if Part II, Division 2 of that Act included the grounds for the refusal to disclose the information set out in subsection (1) of this Act.

(4) Paragraph 102 (3)(a) of the *Access to Information and Protection of Privacy Act, 2015* applies to information referred to in subsection (1) of this section as if the information was information that a head of a public body is authorized or required to refuse to disclose under Part II, Division 2 of that Act.

[2015 cA-1.2 s132](#)

[Back to Top](#)

SNL2014 c23 Amdt.

133. Section 2 of *An Act to Amend the Revenue Administration Act No. 3* is repealed.

[2015 cA-1.2 s133](#)

[Back to Top](#)

SNL2005 cR-15.1 Amdt.

134. Subsection 24(1) of the *Rooms Act* is repealed and the following substituted:

[Back to Top](#)

Restriction

24. (1) A public body that wishes to respond to a request under section 11 of the *Access to Information and Protection of Privacy Act, 2015* with respect to a government record that it intends to transfer to the archives shall transfer that record to the archives with instructions, in writing, that all requests for access to that record be transferred to it in accordance with section 14 of the *Access to Information and Protection of Privacy Act, 2015*, and the *Access to Information and Protection of Privacy Act, 2015* shall apply to that record as if it was still under the care and control of that public body.

[2015 cA-1.2 s134](#)

[Back to Top](#)

SNL2009 cV-6.01 Amdt.

135. Paragraph 41(4)(a) of the *Vital Statistics Act, 2009* is amended by deleting the reference "*Access to Information and Protection of Privacy Act* " and substituting the reference "*Access to Information and Protection of Privacy Act, 2015* ".

[2015 cA-1.2 s135](#)

[Back to Top](#)

Repeal

136. (1) The *Access to Information and Protection of Privacy Act* is repealed.

(2) Sections 4 and 5 of the *Access to Information Regulations, Newfoundland and Labrador Regulation 11/07*, are repealed.

[2015 cA-1.2 s136](#)

[Back to Top](#)

Commencement

137. Subparagraph 2(x)(vi) of this Act comes into force on August 1, 2015.

[2015 cA-1.2 s137](#)

[Back to Top](#)

Schedule A

- (a) sections 64 to 68 of the *Adoption Act, 2013* ;
- (b) section 29 of the *Adult Protection Act* ;
- (c) section 115 of the *Canada-Newfoundland and Labrador Atlantic Accord Implementation Newfoundland and Labrador Act* ;
- (d) sections 90 to 96 of the *Children, Youth and Families Act* ;
- (e) section 5.4 of the *Energy Corporation Act* ;
- (f) section 8.1 of the *Evidence Act* ;
- (g) subsection 24(1) of the *Fatalities Investigations Act* ;
- (h) subsection 5(1) of the *Fish Inspection Act* ;
- (i) section 4 of the *Fisheries Act* ;
- (j) sections 173, 174 and 174.1 of the *Highway Traffic Act* ;
- (j.1) section 21 of the *Innovation and Business Investment Corporation Act*;
- (k) section 15 of the *Mineral Act* ;
- (l) section 16 of the *Mineral Holdings Impost Act* ;
- (m) subsection 13(3) of the *Order of Newfoundland and Labrador Act* ;
- (m.1) sections 10 and 15 of the *Patient Safety Act* ;
- (n) sections 153, 154 and 155 of the *Petroleum Drilling Regulations* ;
- (o) sections 53 and 56 of the *Petroleum Regulations* ;
- (p) [Rep. by 2018 cI-7.1 s24]
- (q) section 12 and subsection 62(2) of the *Schools Act, 1997* ;
- (r) sections 19 and 20 of the *Securities Act* ;
- (s) section 13 of the *Statistics Agency Act* ; and
- (t) section 18 of the *Workplace Health, Safety and Compensation Act* .

[2015 cA-1.2 Sch](#); [2017 cP-3.01 s28](#); [2018 cI-7.1 s24](#); [2018 cC-12.3 s112](#)

[Back to Top](#)

Schedule B

Commission of Inquiry Respecting the Muskrat Falls Project

10/18 s2; [2018 c4 s1](#)

©Queen's Printer



3. Policies

3.1. Email Policy	4
3.2. Information Management and Protection Policy	5


					
Document Title: Email Policy					
Document Type: Policy					No. Of 6
Scope: Government of Newfoundland and Labrador (GNL)					
Trim # DOC15481/2009	Revision (#) 27			Treasury Board Approval (#) TBM2009-298	
Supersedes Email Policy previously approved by TBM 2006-157					
2009-02-03	2009-10-08	2018-02-19	Application and Information Management Services	Office of the Chief Information Officer	Secretary
Date Created	TB Approval Date	Date of last review	Lead Branch - Name	Department	Treasury Board Approval



Table of Contents

1.0	Introduction.....	3
2.0	Purpose.....	3
3.0	Scope.....	3
4.0	Definition and Acronyms.....	3
4.1	Email as a government record.....	4
4.2	Email as a transitory or non-record.....	4
4.3	Management and Retention of E-mail.....	5
4.4	Responsibilities of records creators.....	5
4.5	Public body responsibilities.....	6
5.0	Approval Process.....	6
6.0	Change Process.....	6
7.0	References.....	7



1.0 Introduction

Under the *Management of Information Act*, the Office of the Chief Information Officer (OCIO) has authority for developing and leading the implementation of IM policy and standards for Government; and for providing consultation and advisory services in IM to Government. The Rooms Provincial Archives is mandated, through the *Rooms Act*, to preserve those records of the Government of Newfoundland and Labrador which are deemed to have enduring legal, fiscal, evidential, or research value. Such records are to be preserved regardless of their physical form or characteristics.

Electronic records, like their paper counterparts, need to be recorded, captured in a form which ensures their authenticity and integrity, and made accessible. Electronic records need to provide the same evidence of business activity and the same level of accountability as paper records. Electronic records must also be able to meet the immediate and future needs of organizations, individuals and society. Email, as part of this group of electronic records, needs proper management through appropriate policies and procedures, as well as monitoring and compliance tools.

2.0 Purpose

This policy addresses those email messages which are considered to be “government records” as defined by the *Management of Information Act* making them subject to the same management principles as government records in paper format.

The policy will promote the effective capture, management, and retention of email messages which are government records, in compliance with information management retention requirements.

3.0 Scope

This policy applies to all government departments and public bodies as defined under the *Management of Information Act*.

This policy includes management of email regardless of method of access and use (i.e., use of e-mail via desktop and any wireless mobile devices).

4.0 Definition and Acronyms

Email is defined as messages, including attachments sent and received electronically between personal computers or terminals linked by communications facilities. This includes address information (to, from, cc, bc, subject and date) and the message content.



4.1 Email as a government record

The *Management of Information Act* defines a government record as any record created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and an abandoned record.

Thus, email is a government record when it is created or received in connection with the transaction of Government business. For example, when it records official decisions; communicates decisions about policies, programs and program delivery; or contains background information used to develop other Government documents. Government records may not be destroyed without the authorization of the Government Records Committee, as outlined in the *Management of Information Act*.

When an email is a government record it is subject to legislation such as the *Management of Information Act*, the *Rooms Act*, and the *Access to Information and Protection of Privacy Act, 2015*, and to legal processes such as discovery and subpoena.

Any information transmitted via e-mail and classed as a government record, shall be treated in the same manner as any other important records, in any medium, received or created by a public body. Such records shall be captured into records management systems. As well, electronic messages captured into a records management system are subject to the provisions of the *Management of Information Act*, and shall be scheduled for disposal or retention, as approved by the Government Records Committee, according to the class of records to which they belong.

4.2 Email as a transitory or non-record

Not all messages sent and received via e-mail are government records as defined by the *Management of Information Act*; therefore not all messages are subject to the provisions in the Act. The Act defines a transitory record as a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

Transitory records include:

- Copies of convenience or reference
- Personal messages
- Messages that convey a minor or administrative action (e.g., I will attend the meeting)
- Messages that contain content encapsulated in another record (e.g. exchange of draft documents between collaborators, the content of which is contained in a final report)

Existing transitory records are still discoverable as evidence of Government of Newfoundland and Labrador business activities and are subject to *ATIPPA, 2015* requirements. Retention of transitory records may compound significantly the discovery process as information that should have been destroyed must be processed to the same



standard as other government records in the event of an ATIPP request, audit, inquiry, litigation, etc. Transitory records must be deleted when no longer of value and this may be done without a records retention and disposal schedule.

The employment of appropriate information management principles will ensure that records are kept or destroyed as a routine part of business. If there is doubt about whether a particular type of e-mail is a government record or not, advice should be sought from a Records/Information Management representative in the public body or the Information Management Services Division in the Office of the Chief Information Officer.

4.3 Management and Retention of E-mail

Electronic messages should not be isolated from records and information management systems in the public body. A records management system consists of a set of classifications of records by type and function, sometimes known as records series, and a set of retention periods attached to each type of record. It also includes decisions regarding the final disposition of records, specifically whether, at the end of their life span, they are destroyed or transferred to the Rooms Provincial Archives for permanent retention.

4.4 Responsibilities of records creators:

Email messages, and/or attachments required as evidence of a public body's business activity (i.e. those that are considered official government records), shall be captured using one of the following options. The appropriate procedure(s) is to be determined by the public body.

1. Save the email into an Electronic Document Management System (EDMS) designed specifically for the purpose of managing electronic records; OR
2. Print the message and any applicable attachments to paper and incorporate into the public body's paper records management system; OR
3. Save the message and/or its attachment(s) in a directory outside the email system, which is a part of the public body's official records system (e.g., local area network directory); OR
4. Transmit the message electronically to a central records repository or other appointed representative for incorporation into the public body's records management system

It is undesirable and unnecessary to maintain both electronic and paper copies of emails.

Management of email accounts:

Individual email users are responsible for managing their own email accounts. In addition to the requirements outlined above, email users must keep all login names and passwords confidential in order to protect the security of their records.



Use of e-mail system:

Government's email system is reserved for official Government business, and should not be used for personal purposes. Use of government email for personal financial gain is prohibited. Advertisements which are not work-related are inappropriate and should not be transmitted. The sharing of proprietary software or other copyrighted materials and the distribution of chain letters or other "junk mail" is also unacceptable. Broadcast messages to all users are not permitted except for official Government purposes, through official designates (for example, Communications staff circulating notices on behalf of a department). Email accounts on the government e-mail system are the property of the government and subject to government inspection and review.

Email security:

Any email sent outside the government e-mail system is not secure. Therefore, users should be cautious about the type of message they send outside the Government mail system. Confidential information should not be sent via email outside the Government mail system.

4.5 Public body responsibilities

Public bodies are responsible for ensuring that employees are trained in policies and procedures regarding email use and management. This training can be facilitated through the OCIO.

When an employee is no longer attached to Government it is the responsibility of the Human Resource Division, in cooperation with the employee's immediate supervisor, to notify OCIO personnel. This will ensure the termination of an employee's email account upon departure.

5.0 Approval Process

- Government Records Committee
- Treasury Board - TBM2009-298

6.0 Change Process

This policy will be changed as necessary in order to appropriately reflect current software and media standards and email usage.



7.0 References

Email Guidelines

Instant Messaging Directive

Use of Non-Government Email for Work Purposes

Acceptable Use Directive



Information Management and Protection Policy

GOVERNANCE

Authority:	Treasury Board Approval TBM 2018-111 replaces TBM 2009-335
Applicability:	This Policy provides authority for the OCIO to establish mandatory Information Management and Protection directives and standards for the Government of Newfoundland and Labrador and public bodies supported by the OCIO. The Legislature and the Courts may adopt this policy and any related directives or standards, or develop their own, in keeping with the Management of Information Act.
Compliance Level:	Mandatory
Issuing Public Body:	Office of the Chief Information Officer Moore, Julie Executive Director Application and Information Management Services
Date Issued:	2018-06-04
Date Last Reviewed:	2018-03-29
Version Number:	3.0
OCIO Reference:	DOC18385/2009

Table of Contents

1.0 INTRODUCTION..... 3

2.0 INFORMATION MANAGEMENT AND PROTECTION VISION..... 3

3.0 SCOPE..... 3

4.0 PURPOSE..... 4

5.0 POLICY STATEMENT..... 4

6.0 INFORMATION MANAGEMENT AND PROTECTION PRINCIPLES..... 5

7.0 LEGISLATIVE FRAMEWORK AND AUTHORITY 6

8.0 ROLES AND RESPONSIBILITIES 7

9.0 REVISIONS AND UPDATING 8

GLOSSARY OF TERMS..... 9

1.0 Introduction

The management and protection of information created and collected by the Government of Newfoundland and Labrador and public bodies is subject to the requirements set out in the *Management of Information Act*. The Office of the Chief Information Officer (OCIO) administers this *Act* and in doing so, establishes directives, standards, guidelines and procedures pursuant to this Information Management and Protection Policy.

Any changes required to this policy will be recommended to Treasury Board by the OCIO. Directives and other policy instruments created in association with the Information Management and Protection Policy as outlined below will be developed, disseminated and enforced by the OCIO. The OCIO will use its internal governance mechanisms as well as the Government Records Committee (established under Section 5.1 of the *Management of Information Act*) to receive input and approval for directives and policy instruments.

2.0 Information Management and Protection Vision

A professional Information Management and Protection capability aligned to enable the business of Government, facilitate legislative and policy compliance, appropriately protect the information of Government and citizens and support services to citizens.

3.0 Scope

This policy applies to all government departments and public bodies (hereafter also referred to as “Government”) supported by the OCIO. The Legislature and the Courts may adopt this policy and any related directives or standards, or develop their own, in keeping with the *Management of Information Act*.

This policy framework will:

- Apply to the management and protection of all records (as defined in the *Management of Information Act*) of Government, regardless of physical format or characteristics.
- Apply to all employees and contractors who receive, create or manage information on behalf of the Government.
- Provide the basis for specific Information Management and Protection policies, directives, standards, guidelines and procedures to be developed by the OCIO.

4.0 Purpose

The Information Management and Protection Policy will:

Establish the foundation for development of all Information Management and Protection policies, directives, standards, guidelines and procedures by the OCIO and provide the OCIO with a comprehensive approach in addressing Information Management and Protection Policy governance.

5.0 Policy Statement

The Government of Newfoundland and Labrador manages and protects information in accordance with the *Management of Information Act* (specifically *Section 6*), the *Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)* and through this policy and associated policy instruments such as directives, guidelines and procedures.

Records in all formats must be managed and protected throughout their lifecycle by any employee or contractor who creates or collects the record as part of their responsibility in performing work for Government.

Records and information must be protected from unauthorized access. Physical and technical means must be applied, as appropriate to the level of sensitivity of the information, taking into consideration requirements to preserve confidentiality, support availability and protect the integrity of the information.

Anyone who willfully collects, uses or discloses (i.e. breaches) personal information in contravention of *ATIPPA, 2015* may be subject to penalty under Section 115(1) of that Act and/or consequences under the appropriate personnel policy of Government, up to and including dismissal, depending upon the severity of the breach.

Breaches of personal and/or confidential information may be subject to consequences under the appropriate personnel policy of Government, up to and including dismissal, depending upon the severity of the breach.

Policy instruments, as outlined below, may be established and enforced by the OCIO under the authority provided through this policy.

Information Management and Protection Policy Instruments:

Policy – a policy is a high level, strategic statement, authorized by the executive management that dictates what type of position the organization has taken on specific issues. Treasury Board approval of Government-wide policy is required, except for policies established by the Legislature and the Courts. Treasury Board approved policies are recognized by all Government departments and compliance with them by departments is mandatory.

Directive – directives provide specific direction to Government and derive their authority from the “Information Management and Protection Policy”. The OCIO has the authority to develop and release directives upon internal review and approval by the OCIO Security Council in the case of Information Protection directives. The Government Records Committee will review and approve Information Management directives. Compliance with OCIO directives is mandatory, except if the Legislature or the Courts are determined, through their own governance and authority, to be exempt.

Standard – standards are generally mandatory requirements that support individual policies and directives and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. They may be internal to the OCIO, or meant to be used across all of Government. The OCIO has the authority to develop and release standards upon internal review and approval by the OCIO Security Council in the case of Information Protection standards. The Government Records Committee will review and approve Information Management standards. Compliance with OCIO standards may be mandatory or optional if the Legislature or the Courts are determined, through their own governance and authority, to be exempt.

Guideline – guidelines represent recommended actions, general approaches and operational behaviours. Guidelines are not mandatory. They are often used as templates to write procedures. Guidelines support policy and directives by providing a “how to” approach. They may be internal to the OCIO or meant to be used across all of Government. The OCIO has the authority to develop and release guidelines upon internal review and approval by the OCIO Security Council in the case of Information Protection standards. The Government Records Committee will review and approve Information Management guidelines. Compliance with OCIO guidelines is not mandatory.

Procedure – a procedure is a detailed step-by-step, task-level definition of actions required to achieve a certain result. The procedure answers the "How" question and is generally used in an operating environment. They may be internal to the OCIO or meant to be used across all of Government.

6.0 Information Management and Protection Principles

The OCIO is guided by the relevant International Standards Organization (ISO) and Canadian General Standards Board (CGSB) standards for its policy development framework and overall approach. The development of Information Management and Protection policies, directives, standards and guidelines by the OCIO is based upon the following principles:

Promoting records creation to support the conduct of business, comply with the regulatory environment and provide necessary accountability.

Enabling transparency of decision-making and expenditure through the development of proper information management and protection practices throughout Government operations and systems, and the appropriate training of information management personnel to provide effective service delivery.

Enabling legislative compliance where a requirement to retain records is articulated or where legislative compliance relies upon timely and appropriate access to information resources.

Lifecycle management of all information in all formats during all lifecycle stages from creation (through use and management) to disposal (through destruction, deletion or transfer to The Rooms Corporation, Provincial Archives Division for permanent preservation).

Providing information authenticity, integrity and security to protect information holdings from loss, inappropriate access or use, disclosure, alteration, removal or destruction; thereby ensuring confidentiality, integrity, availability and accountability over time.

Risk management through the assurance that security risks are identified, acceptable and that control mechanisms are in place.

7.0 Legislative Framework and Authority

The OCIO, as directed by Section 5 of the *Management of Information Act*, is accountable to:

- Develop and implement a management program for government records in the province.
- Provide advice to and assist public bodies with developing, implementing and maintaining record management systems.
- Recommend policies to Treasury Board for adoption.

The *Management of Information Act* (Section 5.1) also establishes the Government Records Committee, which has a mandate to make recommendations to the Minister respecting record retention, disposal and transfer to The Rooms Corporation, Provincial Archives Division.

8.0 Roles and Responsibilities

Groups	Responsibilities
Office of the Chief Information Officer (OCIO)	<ul style="list-style-type: none"> • Defines and publishes Information Management and Protection policies, directives, standards and guidelines. • Responsible for the Information Management and Protection policies, directives, standards and guideline documentation, and identifies requirements for updating and modification as required. • Ensures appropriate communications regarding Information Management and Protection policies, directives, standards and guidelines takes place. • Manages, maintains and monitors the policies, directives, standards and guidelines for effectiveness and compliance.
OCIO Security Council	<ul style="list-style-type: none"> • Approve and/or recommend policies, directives, standards, guidelines and procedures for information protection and security. • Address information protection and security issues as required either to ensure adherence to the OCIO’s Information Protection and Security Framework and Strategy or to recommend changes as required to the OCIO Senior Leadership Team (SLT).
Government of Newfoundland and Labrador Departments and Public Bodies (“Government”)	<ul style="list-style-type: none"> • Comply with the Information Management and Protection policies, directives, standards and guidelines (except in cases where the Legislature or the Courts may be determined to be exempt). • Comply with Section 6 of the <i>Management of Information Act</i>, which states: ‘a permanent head of a public body shall develop, implement and maintain a record management system.’ • Develop departmental or organizational procedures complementary to the policies, directives, standards and guidelines.
Government employees and contractors	<ul style="list-style-type: none"> • Comply with the Management of Information Act and the Access to Information and Protection of Privacy Act, 2015. • Comply with the Information Management and Protection Policy.
Cabinet Secretariat	<ul style="list-style-type: none"> • Responsible for policy direction for Cabinet Records in accordance with Section 5.4 (1) of the <i>Management of Information Act</i>.

Groups	Responsibilities
Treasury Board	<ul style="list-style-type: none"> • Approves Government of Newfoundland and Labrador policies.
Government Records Committee	<ul style="list-style-type: none"> • Reviews Information Management and Protection policies, directives, standards and guidelines and makes recommendations to the Minister as required. • Approves Information Management directives, standards, guidelines and procedures.
Information Management (IM) Directors' Forum	<ul style="list-style-type: none"> • Reviews Information Management and Protection policies, directives, standards and guidelines. • Advises the OCIO on matters related to Information Management.
Access to Information and Protection of Privacy (ATIPP) Office	<ul style="list-style-type: none"> • Advises and educates public bodies on the appropriate and consistent application of the ATIPP Act, 2015. • Supports ATIPP Coordinators in public bodies. • Develops policy, procedures and standards. • Maintains and reports statistics. • Reviews policies and policy instruments having relevance to access to information and privacy of personal information.
The Rooms Corporation, Provincial Archives Division	<ul style="list-style-type: none"> • Reviews policies and policy instruments dealing with the identification of archival and non-archival records. • Responsible for the long term preservation of records with archival value as per the Rooms Act and for making these records available for research.

9.0 Revisions and Updating

This policy will be reviewed and updated as required. Incidental revisions which may be required from time to time as a result of changes in operational requirements, legislation or other policies, will be made in a timely manner as necessary and submitted for approval to Treasury Board.

APPENDIX

Glossary of Terms

AVAILABILITY - Availability is the property of being accessible and useable upon demand by an authorized entity (Source: ISO 13335-1:2004). It is the ability of a component or service to perform its required function at a stated instant or over a stated period of time. Availability is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the customers within the agreed service hours (Source: Information Technology Infrastructure Library (ITIL)).

AUTHENTICITY - An authentic record is one that can be proven:

- To be what it purports to be;
- To have been created or sent by the person purported to have created or sent it;
- To have been created or sent at the time purported (Source: ISO 15489:2001).

CABINET RECORDS - include memoranda to Cabinet for the purpose of presenting proposals or recommendations; discussion papers, policy analysis, proposals, advice or briefing material, including all factual and background material prepared for Cabinet; agendas, minutes or other records recording deliberations or decisions of Cabinet; communications or discussions among ministers on matters relating to the making of Government decisions or the formulation of Government policy; records created for or by a minister for the purpose of briefing that minister on a matter for Cabinet; records created during the process of developing or preparing a submission for Cabinet; draft legislation or regulation; or information about the contents of a Cabinet Record. - [Management of Information Act](#)

CONFIDENTIAL INFORMATION - The working definition of “confidential information” includes, but is not necessarily limited to the following types of information:

- Cabinet Records as defined in the *Management of Information Act*
- Draft legislation, policies and procedures
- Legal opinions
- Communications plans and collateral materials (e.g., draft news releases, Qs and As)
- Sensitive reports, strategies or proposals under development
- Planning documents
- Trade secrets or 3rd party business information submitted in confidence

As a general rule, any information which would be exempt from public access under the *Access to Information and Protection of Privacy Act, 2015* should be considered confidential.

GOVERNMENT RECORDS COMMITTEE (GRC) - The Government Records Committee is the official body that is mandated to:

- Review and revise schedules for the retention, disposal, destruction or transfer of government records;
- Make recommendations to the minister respecting public records to be forwarded to The Rooms Corporation, Provincial Archives Division;
- Authorize disposal and destruction standards and guidelines for the lawful disposal and destruction of government records;
- Make recommendations to the minister regarding the removal, disposal and destruction of records (*Management of Information Act*).

INFORMATION MANAGEMENT - Information management (IM) is a program of records and management of information practices instituted to provide an economical and efficient system for the creation, maintenance, retrieval and disposal of government records. Under the *Management of Information Act*, the permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records.

INFORMATION PROTECTION - Information protection (IP) is an area of practice focused on the protection of information from inappropriate access or use, using a variety of means, including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. IP represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, public bodies are required to protect information as part of their accountability under Section 6 of the [Management of Information Act](#).

INTEGRITY - Integrity demonstrates that the record is complete and has been unaltered. It is necessary that a record be protected against unauthorized alteration. (Source: ISO 15489:2001).

LIFECYCLE - The life cycle refers to the stages through which information is managed. Information management strives to manage the records in a manner that facilitates authenticity, reliability, integrity and usability throughout all stages including:

- Planning;
- Creation and organization;
- Receipt and capture of data;
- Retrieval, processing, dissemination and distribution of data;
- Storage, maintenance and protection;
- Archival preservation or destruction or expungement (Source: CAN/CGSB-72.34-2005).

OCIO SECURITY COUNCIL - the OCIO Security Council is a governance body of the OCIO consisting of Director-level representatives from all OCIO branches. Its mandate is to oversee the effectiveness of the OCIO's Information Security Strategy and to recommend policies and procedures for information protection and security. It also addresses information protection and security issues as required to either ensure adherence to the OCIO's Information Protection and Security Framework and Strategy or to recommend changes as required to the Senior Leadership Team (SLT).

PERSONAL INFORMATION - Personal information means recorded information about an identifiable individual, including:

- The individual's name, address or telephone number;
- The individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
- The individual's age, sex, sexual orientation, marital status or family status;
- An identifying number, symbol or other particular assigned to the individual;
- The individual's fingerprints, blood type or inheritable characteristics;
- Information about the individual's health care status or history, including a physical or mental disability;
- Information about the individual's educational, financial, criminal or employment status or history;
- The opinions of a person about the individual;

- The individual's personal views or opinions, except where they are about someone else; (*Access to Information and Protection of Privacy Act, 2015*).

PUBLIC BODY – a public body is a department created under the *Executive Council Act* or a branch of the executive government of the province, a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown, a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an *Act* of the province, the Lieutenant-Governor in Council or a minister of the Crown, a court established under an *Act* of the province, or the House of Assembly and committees of the House of Assembly - [Management of Information Act](#)

RECORD - means a correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic - [Management of Information Act](#)



4. Directives

4.1. Instant Messaging	7
4.2. Acceptable Use of the Government Network and/or IT Assets	8
4.3. Use of Non-Government Email Accounts for Work Purposes	9



Government of Newfoundland and Labrador
Office of the Chief Information Officer
Application and Information Management Services Branch

DIRECTIVE – INSTANT MESSAGING

Directive (Definition): OCIO Directives derive from Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335). The OCIO directives are mandatory for users to follow. Directives are supported by Standards and Guidelines, where applicable

Authority	Treasury Board Approval TBM 2018-111 (replaces TBM 2009-335)
Issuing Branch	Application and Information Management Services Branch Information Management Services Division
Target Audience	This Directive applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the Government of Newfoundland and Labrador (hereafter referred to as individuals).
Compliance Level	Mandatory
Issue Date	2012-02-01
Last Review Date	2018-09-24
OCIO Reference	DOC00967/2012

APPROVAL AND SIGN OFF

Office of the Chief Information Officer	Julie Moore, Executive Director Application and Information Management Services
--	--

VERSION 3.0

Table of Contents

1.0 OVERVIEW..... 3

2.0 PURPOSE..... 3

3.0 SCOPE..... 3

4.0 DIRECTIVE STATEMENTS 3

5.0 ROLES AND RESPONSIBILITIES 4

6.0 DEFINITIONS AND ACRONYMS..... 5

7.0 COMPLIANCE AND ENFORCEMENT 6

8.0 MONITORING AND REVIEW..... 6

9.0 REFERENCES..... 6

1.0 Overview

Instant messaging technologies are designed to support real-time conversational interactions and are commonly used to facilitate the flow of business. Typically, they replace a conversation that previously occurred in person or over the phone. These technologies provide a temporary space for an electronic conversation (instant message) to occur. Instant messages are subject to legal, audit and responsive to access to information requests and must be managed appropriately. Therefore, where they record government business activities, instant messages must be retained. The information owner must ensure it is converted to a recordkeeping format and managed appropriately.

2.0 Purpose

This Directive provides individuals (as defined later in section 6.0), OR information owners with information management requirements for the use of instant messaging technologies including:

- Applications or tools accessible through the Government of Newfoundland and Labrador's Information Technology (IT) network.
- Any device capable of generating instant messages (e.g., computers, smart phones, tablets and other mobile communication devices).

3.0 Scope

This Directive applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the Government of Newfoundland and Labrador (hereafter referred to as individuals).

4.0 Directive Statements

- a) Instant messages must be treated like any other information resource and managed according to the *Management of Information Act*.
- b) Individuals are responsible for managing the information they create, receive, or transmit in instant messages.
- c) Instant messages are subject to legal, audit and responsive to *Access to Information and Protection of Privacy Act, 2015* requests.

- d) Instant messages that do not record government business are transitory, and must be deleted as soon as possible, unless an information request has been received.
- e) It is the responsibility of the information owner to transfer instant messages to a proper government recordkeeping system where required.

5.0 Roles and Responsibilities

Individuals

- Understand requirements for managing and protecting information.
- Appropriately use instant messaging technologies supported by the OCIO.
- Ensure that instant messages are regularly deleted from devices which retain them.
- Transfer any instant messaging communication that constitutes a government record to an appropriate recordkeeping format so that it can be managed according to the requirements for managing government records set out in the *Management of Information Act*.

Office of the Chief Information Officer (OCIO)

- Support authorized instant messaging technologies.
- Maintain the Instant Messaging Directive and any associated supporting materials.
- Provide education and awareness on the use of instant messaging technologies.

Managers and Directors within a Public Body

- Ensure all individuals within the program or service area of responsibility are aware of this Directive and related guidelines.
- Ensure individuals have proper approval and training on this Directive.

Information Management Division or Equivalent within a Public Body

- Provide direction on this Directive.
- Provide direction to individuals on appropriate storage of converted instant messages in the records management system or in other approved locations.

Deputy Minister or Permanent Head of a Public Body or Designate

- Administer this Directive across their Department or Public Body.

6.0 Definitions and Acronyms

Individual (as it relates to this document)– all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the Government of Newfoundland and Labrador, including all public bodies as defined under the *Management of Information Act*.

Instant Message - An instant message is a form of real-time direct text-based communication also known as an electronic conversation between two or more people using personal computers or other devices and conveyed over a network, such as the Internet.

Government Record - Government records are records created by or received by a public body in the conduct of its affairs and includes Cabinet records, transitory records and abandoned records. Disposal of a government record must be sanctioned by a records retention and disposal schedule that has been approved by the Government Records Committee (GRC).

Transitory Record - A transitory record is a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can be securely destroyed when no longer of value without authorization of the Government Records Committee (GRC).

Public Body (as defined under the *Management of Information Act*)

- i) a department created under the *Executive Council Act* or a branch of the executive government of the province,
- ii) a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown,
- iii) a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a minister of the Crown,
- iv) a court established under an Act of the province, and
- v) the House of Assembly and committees of the House of Assembly;

7.0 Compliance and Enforcement

Mandatory compliance - OCIO directives are mandatory for individuals to follow and dictate uniform ways of operating.

Compliance monitoring - Compliance monitoring of this Directive is the responsibility of the Public Body.

Penalty for failure to comply - Failure to comply with this Directive, or contravention through negligence, may result in disciplinary action, up to and including termination of employment or other disciplinary action as per the policies and procedures established by Treasury Board. Human Resource Policies can be accessed through the following link: http://www.exec.gov.nl.ca/exec/hrs/working_with_us/policies.html.

8.0 Monitoring and Review

The Application and Information Management Services Branch is responsible for monitoring and reviewing this Directive in accordance with processes set forth as per the Information Management and Protection Policy.

9.0 References

Management of Information Act

<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)

https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.pdf

Human Resource Policies

http://www.exec.gov.nl.ca/exec/hrs/working_with_us/policies.html

Executive Council Act

<http://assembly.nl.ca/Legislation/sr/statutes/e16-1.htm>

Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)

<http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm>



DIRECTIVE – ACCEPTABLE USE OF THE GOVERNMENT NETWORK AND/OR INFORMATION TECHNOLOGY ASSETS

Directive (Definition): Information Protection and Security (IP&S) directives derive from the [Information Management and Protection Policy, TBM 2018-111 \(replaces TBM 2009-335\)](#) approved by Treasury Board. IP&S directives are mandatory for users to follow. Directives are supported by standards and guidelines, where applicable.

Issuing Branch	Operations and Security Branch <i>Information Protection Division</i>
Target Audience	All Government departments and public bodies supported by the OCIO
Approval Date	December 2018
Review Period	Every 3 Years
Last Review Date	September 2018
Next Review Date	September 2021
Related Standards	Not Applicable
Related Guidelines	Not Applicable

APPROVAL AND SIGN OFF

OCIO Senior Leadership Team (SLT)	<i>Approver of IP&S Directives</i>
OCIO Security Council	<i>Approver of IP&S Standards and Guidelines</i>

VERSION 2.0

TABLE OF CONTENTS

1.	Overview	3
2.	Purpose and Scope	3
3.	Definitions and Acronyms	3
4.	Acceptable Use Statements	4
5.	Monitoring of the Network and IT Assets.....	4
6.	Roles and Responsibilities	5
7.	Compliance and Enforcement	5
8.	Directive Monitoring and Review.....	5
9.	References.....	6
10.	Revision History.....	6

ACCEPTABLE USE OF THE GOVERNMENT NETWORK AND/OR INFORMATION TECHNOLOGY ASSETS

DIRECTIVE

1. Overview

Access to and use of Government of Newfoundland and Labrador (hereafter referred to as ‘Government’ or ‘the Employer’) Information Technology (IT) resources and assets is provided for the sole purpose of conducting Government business and performing work-related activities. It is critical that the Government Network (hereafter referred to as ‘the Network’) and Government IT assets are protected from unauthorized or inappropriate access or use. Inappropriate access or use of the Network and/or Government IT assets, either knowingly or unknowingly, exposes the Employer to risks that may compromise the protection, security and performance of its information, IT systems and services.

The Network, its components and all Government IT assets are the property of the Employer and not the property of the employee. As such, employees should be aware these assets, equipment and resources are monitored and will be searched where necessary for the maintenance or security of the Network and government’s overall IT environment, or if inappropriate use is suspected, by those authorized to do so on behalf of the Employer or law enforcement agencies.

2. Purpose and Scope

The purpose of this Directive is to clearly identify acceptable use of the Network and any Government IT assets, including but not limited to computers; mobile devices such as laptops, smartphones and tablets; applications; software; electronic storage devices; servers; printers; and shared drives. This Directive applies to IT assets owned by the Government or devices approved for use on the Network.

This Directive applies to all Government departments and public bodies supported by the OCIO; it is mandatory to follow this Directive.

3. Definitions and Acronyms

Employee – In the context of this Directive, ‘Employee’ includes staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons entrusted to access or use the Network and/or IT assets on behalf of the Employer.

Network – A series of computers and other technology devices that facilitates communications and allows for the sharing of information and resources across an organization, including both wired and wireless technologies.

IT Assets – Technology components of an organization such as computers, mobile devices, software, hardware, applications, electronic storage devices, servers, printers and shared drives that have value to the organization.

Information Protection (IP) – An area of practice focused on the protection of information from inappropriate access or use, using a variety of means as required; including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. IP represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, public bodies are required to protect information as part of their accountability under Section 6 of the [Management of Information Act SNL2005 c.M-1.01](#).

Mobile Device – A portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) (Source: NISTSP 800-53).

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means (Source: NIST SP 800-83). Phishing is a type of fraud that uses deceptive e-mails, websites and/or text messages to gather personal, financial and confidential information for fraudulent purposes and/or unauthorized access.

Smartphone – An ‘all in one’ mobile phone (e.g., Blackberry, iPhone, etc.) with an underlying operating system that runs applications and software to provide advanced functionality, similar to a computer (e.g., Internet access, email, videos, music, photos, document editing, etc.).

Software – Application and system programs that provide instructions and directions to computers and other technology devices.

SPAM - Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages (Source: NIST CNSSI-4009).

Tablet – A wireless, portable, lightweight computer with a touchscreen interface (e.g., iPad).

Virus - A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk (Source: NIST CNSSI-4009).

4. Acceptable Use Statements

- 1) Employees must securely manage and protect any Government IT assets in their use;
- 2) Employees must not use the Network or Government IT assets for illegal or criminal purposes or to contravene legislation, policies, directives or standards;
- 3) Employees must not initiate or participate in any activity that negatively impacts the Network's security or performance;
- 4) Employees must not gain or attempt to gain unauthorized access to, or circumvent the security controls of, the Network or Government IT assets;
- 5) Employees must not spread or attempt to spread viruses, SPAM or other malicious content with intent to cause harm to the Network or Government IT assets;
- 6) Employees must take reasonable precautions to prevent the introduction of viruses, SPAM or other malicious content into or on the Network or Government IT assets;
- 7) Employees must only use Government-approved and OCIO managed mobile devices on the Network;
- 8) Employees must only install licensed software on Government IT assets;
- 9) Employees must only install Government-approved hardware on the Network;
- 10) Employees must securely manage and protect the usernames and passwords they use on the Network or Government IT assets;
- 11) Employees must not use the Network or Government IT assets for personal use that interferes with their performance of work-related duties;
- 12) Employees must not use Network file shares for non-Government purposes;
- 13) Employees must not use the Network or Government IT assets for personal gain or for any unauthorized commercial purposes;
- 14) Employees must immediately notify the OCIO IT Service Desk (servicedesk@gov.nl.ca or 709-729-HELP) if they know of or suspect potential harm to the Network or any Government IT assets (e.g., stolen laptop, viruses, SPAM, phishing, compromised user credentials);
- 15) Employees must return any Government IT assets to a manager or direct supervisor upon departure from the Government;
- 16) Departments must notify the OCIO IT Service Desk in a timely manner of departing employees (e.g., due to retirement, transfer, dismissal, leave of absence, etc.); and
- 17) The Employer and Employees must be aware of any legislation, policies, directives, standards and guidelines related to the management, protection and security of Government information. Refer to Section 9 of this Directive, the OCIO's [Information Management and Protection website](#) and employees should engage the Director responsible for information management within their department.

5. Monitoring of the Network and IT Assets

The Network, its components and all Government IT assets are the property of the Employer and not the property of the Employee. The Employer can add, remove, update and/or block any content, technical or

otherwise, and view all Government records (as well as any other records which may be generated, stored on or handled by Government-issued assets), if that action is deemed necessary for the maintenance or security of the Network, or if inappropriate use is suspected. The Employer maintains the right to monitor the Network, its components and all Government IT assets for the purposes of maintenance, repair and management; to ensure continuity of service; to improve business processes and productivity; to meet its legal requirement to produce information; and to prevent misconduct and ensure compliance with the law. The Employer may forward IT assets and/or information to law enforcement agencies when deemed necessary.

Employees should be aware these assets, equipment and resources are monitored and will be searched where necessary for the maintenance or security of the Network and government's overall IT environment, or if inappropriate use is suspected, by those authorized to do so on behalf of the Employer or law enforcement agencies.

6. Roles and Responsibilities

Office of the Chief Information Officer (OCIO)

- Develop, implement and maintain this Directive
- Oversee education and awareness of this Directive across Government
- Monitor and manage the Network and Government IT assets, as required
- Approve mobile devices and hardware that can connect to and/or be used on the Network

Employees

- Be aware of the responsibilities as outlined in this Directive
- Be aware of the requirements for Information Management and Protection
- Adhere to this Directive and any related legislation, policies, directives or standards

Departments

- Notify the OCIO IT Service Desk of departing employees

Deputy Ministers (or Equivalent)

- Enforce this Directive across their Department or Public Body

7. Compliance and Enforcement

Mandatory compliance

Adherence to this Directive is mandatory for all employees.

Enforcement

Enforcement of this Directive is the responsibility of the Deputy Minister or equivalent of each department or public body, as per the *Management of Information Act*, and the *Information Management and Protection Policy* as approved by Treasury Board, under which it is issued. Where necessary, enforcement will be undertaken by the OCIO in accordance with requirements to secure the Government Network and Government issued and owned IT assets.

Penalty for failure to comply

Willful non-compliance with this Directive, including contravention through negligence, may result in disciplinary action by the Employer, up to and including termination of employment, in accordance with Government's [human resource policies](#).

8. Directive Monitoring and Review

The OCIO is responsible for monitoring and reviewing the content of this Directive. For clarification of this Directive, contact OCIOInfoProtection@gov.nl.ca.

9. References

Management of Information Act

<http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Information Management and Protection Policy (TBM 2018-111 which replaces TBM 2009-335)

https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.html

Equipment and Resource Usage Policy

http://www.exec.gov.nl.ca/exec/pss/working_with_us/equipment_and_resources.html

Password Management Best Practices

http://www.ocio.gov.nl.ca/ocio/im/employees/pdf/password_management_bp.pdf

Human Resource Policies

http://www.exec.gov.nl.ca/exec/hrs/working_with_us/policies.html

Directive – Mobile Devices for Government Employees

http://www.ocio.gov.nl.ca/ocio/publications/policies/Directive_Mobile_Devices_for_Government_Employees.pdf

FYI – Information Protection in the Workplace – Tops Tips for Protecting Government Information

[http://www.ocio.gov.nl.ca/ocio/im/practitioners/Information_Protection_IP_in_the_Workplace_\(Top_Tips\).pdf](http://www.ocio.gov.nl.ca/ocio/im/practitioners/Information_Protection_IP_in_the_Workplace_(Top_Tips).pdf)

FYI - Phishing – Don't Get Caught

<https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/Phishing.pdf>

OCIO's Information Management and Protection website

<https://www.ocio.gov.nl.ca/ocio/im/index.html>

10. Revision History

December 2018	Version 2.0
January 2015	2 Year Review Completed (No Updates Required)
January 9, 2013	Version 1.0



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Corporate and Information Management Services Branch

DIRECTIVE – USE OF NON-GOVERNMENT EMAIL ACCOUNTS FOR WORK PURPOSES

Directive (Definition): OCIO Directives derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. The OCIO directives are mandatory for users to follow. Directives are supported by Standards and Guidelines, where applicable.

Issuing Branch	Corporate and Information Management Services
Approval Date	2016-12-06

APPROVAL AND SIGN OFF

Chief Information Officer	Ellen MacDonald		
	(name)	(signature)	(date)
Executive Director, Issuing Branch	Julie Moore		
	(name)	(signature)	(date)
Executive Director, Corporate and Information Services Branch	Julie Moore		
	(name)	(signature)	(date)

Note: Questions related to this policy should be forwarded to OCIO@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	3
2.0	Purpose.....	3
3.0	Scope.....	3
4.0	Directive Statements	3
5.0	Roles and Responsibilities	4
6.0	Definitions and Acronyms.....	5
a)	Definitions.....	5
b)	Acronyms.....	5
7.0	Compliance and Enforcement	6
8.0	Monitoring and Review	6
9.0	References.....	6

USE OF NON-GOVERNMENT EMAIL ACCOUNTS FOR WORK PURPOSES

DIRECTIVE

1.0 Overview

The *Management of Information Act (MOIA)* requires Public Bodies to manage and protect government records regardless of format, this includes email. These records exist to document and support the activities of the public body and to support transparency and accountability of government. Individuals provided with a government-issued email account are expected to use it for business purposes. Use of a non-government email account to conduct work on behalf of a public body is not permitted.

2.0 Purpose

This Directive mandates the individual's responsibility related to the use of non-government email accounts.

3.0 Scope

This Directive applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons (herein referred to as individuals) working on behalf of the Government of Newfoundland and Labrador or a Public Body.

4.0 Directive Statements

- a) Individuals must adhere to the [Email Policy, Email Guidelines and Best Practices](#) established by the OCIO as well as those established by the Public Body to which they report.
- b) Use of a personal or non-government email account to conduct work on behalf of a Public Body is not permitted.
- c) The Permanent Head of the Public Body or Designate can make exceptions to this Directive in limited, identified cases where the requirement and nature of the information exchanged is well understood and a clear process to transfer government records to an approved government storage location (e.g. government email account, network drive, paper file, etc.) has been established. In these cases, the exceptions must be clearly approved and documented.
- d) If an individual inadvertently receives an email on their personal or non-government account that involves government business, they must copy or forward the email to their official organizational account as soon as possible.

The record will then be saved to an approved storage location (e.g. government email account, network drive, paper file, etc.). This will ensure the record is returned to the proper custody and control of government, supporting the security and accessibility of that record.

- e) Once transferred to an appropriate government location, the initial email should be immediately deleted from the individual's personal or non-government email account including the sent mail folder.
- f) Individuals may forward email from their government-issued account to a personal or non-government email account under either of the following conditions:
 - o Use of the non-government account for government work purposes has been specifically approved by the head of the public body or approved designate to whom the individual reports.
 - o Content is clearly intended to be publicly available including content the public body, prints, publishes or releases for general or limited distribution to the public.
 - o Email of a personal nature that is either not work related or pertains to the individual's relationship with the public body as an employer (e.g. leave reports, HR records, etc.).
- g) External public bodies that do not avail of government IT services should work with the department to which they report to discuss their current organizational standards for managing email and any required exceptions to this Directive.
- h) External public bodies with their own email system should ensure external entities working on their behalf follow this Directive.

5.0 Roles and Responsibilities

Individuals

- Adhere to this Directive and any related legislation, policies, directives or standards.

Public Body Managers and Directors

- Ensure all individuals within the program or service area of responsibility are aware of this Directive and related guidelines.
- Ensure individuals have proper approval and training on this Directive.

Information Management Division or Equivalent within a Public Body

- Provide direction on this Directive.
- Provide direction to individuals on appropriate storage of email in the records management system or in other approved locations.

Deputy Minister or Permanent Head of a Public Body or Designate

- Administer this Directive across their Department or Public Body.
- Ensure a process for exceptions from the Directive has been established.

OCIO

- Develop, implement and maintain this Directive.
- Oversee education and awareness of this Directive across government.

6.0 Definitions and Acronyms

a) Definitions

Transitory Record - A transitory record is a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can be securely destroyed when no longer of value without authorization of the Government Records Committee (source: [Management of Information Act SNL2005 c.M-1.01](#)).

Record – A record means a correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic (Source: [Management of Information Act SNL2005 c.M-1.01](#)).

Government Record - A government record is a record created by or received by a public body in the conduct of its affairs and includes a Cabinet record, transitory record and an abandoned record. (source: [Management of Information Act SNL2005 c.M-1.01](#)).

Public Body - A "public body" means:

- (i) a department created under the *Executive Council Act* or a branch of the executive government of the province,
 - (ii) a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown,
 - (iii) a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a minister of the Crown,
 - (iv) a court established under an Act of the province, and
 - (v) the House of Assembly and committees of the House of Assembly
- (source: [Management of Information Act SNL2005 c.M-1.01](#)).

b) Acronyms

IM	Information Management
MOIA	Management of Information Act
OWA	Outlook Web Access

7.0 Compliance and Enforcement

Mandatory compliance

OCIO directives are mandatory for individuals to follow and dictate uniform ways of operating.

Compliance monitoring

Compliance monitoring of this Directive is the responsibility of the Public Body.

Penalty for failure to comply

Failure to comply with this Directive, or contravention through negligence, may result in disciplinary action, up to and including termination of employment or other disciplinary action as per the policies and procedures established by Treasury Board. Human Resource Policies can be accessed through the following link: http://www.exec.gov.nl.ca/exec/hrs/working_with_us/policies.html.

8.0 Monitoring and Review

The Corporate and Information Management Services Branch is responsible for monitoring and reviewing this Directive in accordance with processes set forth as per the Information Management and Protection Policy.

9.0 References

[Management of Information Act](#)

[Information Management and Protection Policy](#)

[Email Policy](#)

[Acceptable Use of the Government Network and Information Technology Assets](#)



5. Standards

5.1. Developing One Time Disposal Submissions	11
5.2. Developing RRDSs for Operational Records	12
5.3. Corporate Records Information Management Standard	13



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

STANDARD – DEVELOPING ONE TIME DISPOSAL SUBMISSIONS

Standard (Definition): OCIO Standards derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. The OCIO standards are mandatory for users to follow and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. Standards are usually defined to support the policies and directives and are supported by Guidelines, where applicable.

Issuing Branch	Information Management Branch
Approval Date	<i>February 10, 2015</i>
Authorizing Directive <i>(Where applicable)</i>	
Authorizing Body	Government Records Committee
GRC Approval Meeting Number	GRC Meeting 2015-002

APPROVAL AND SIGN OFF

Secretary, Government Records Committee Coordinator, GRLM CIMS, OCIO	Kimberly Porter
	(name) (signature) (date)
Chair, Government Records Committee Director, IM CIMS, OCIO	Iris Power
	(name) (signature) (date)

Note: Questions related to this standard should be forwarded to OCIO@gov.nl.ca

CONFIDENTIAL While in Draft – Limited Distribution

TABLE OF CONTENTS

1.0	Overview	3
2.0	Purpose.....	3
3.0	Scope.....	3
4.0	Required Approach	3
4.1	Completing the One Time Disposal Submission.....	3
4.1.1	Number of Boxes	4
4.1.2	Record Series Title	5
4.1.3	Records Created By Department/Public Body/Branch/Division.....	5
4.1.4	File Date Range.....	5
4.1.5	Custodian/Contact Person	5
4.1.6	Departmental or Public Body Access and Privacy Coordinator	5
4.1.7	ATIPP Exceptions	5
4.2	Submitting One Time Disposal Submission for Review and Approval.....	6
5.0	Definitions and Acronyms.....	6
5.1	Definitions.....	6
5.2	Acronyms.....	7
6.0	Compliance and Enforcement	7
7.0	Monitoring and Review	7
8.0	References.....	7
9.0	Revision History	7
	Appendix A: One Time Disposal Submission Template	8
	Appendix B: Template Memorandum for One Time Disposal Submission to the Government Records Committee	9
	Appendix C: Government of Newfoundland and Labrador Records Disposal Process.....	10
	Appendix D: One Time Disposal Submission Checklist	11
	Appendix E: Sample File Listing	12

DEVELOPING ONE TIME DISPOSAL SUBMISSIONS

STANDARD

1.0 Overview

Records disposal in the Government of Newfoundland and Labrador refers to authorized removal of records by means of destructions, transfer to The Rooms Provincial Archives Division (TRPAD) for permanent preservation, or transfer to another entity. Disposal of records can only be carried out in one of three ways; as part of implementing approved records retention and disposal schedules: as a result of a destruction request authorized by the Government Records Committee (GRC); or as an authorized transfer of records to another entity. The disposal of government records must be authorized by the GRC as per the *Management of Information Act*. The *Management of Information Act* mandates the Government Records Committee (GRC) to make recommendations to the Minister relating to the disposal of government records.

A One Time Disposal (OTD) submission is a mechanism whereby a department can apply to the GRC for their permission to dispose of records. It is not meant to be a replacement for the regular and consistent implementation of a Records Retention and Disposal Schedule (RRDS). It may be used when records have resulted from an activity no longer in progress (e.g. organizational unit, service or function that no longer exists, or business function or project which was created to suit a specific purpose and had a specific lifespan). It may apply to records in any format, and can be for the records of a specific branch or division. It can encompass all types of records within an organization, or may be limited to specific record types or record series. A One Time Disposal Submission is used to dispose of a backlog of inactive records not covered under a retention schedule.

The process includes an inventory of records, volume of records in question and the submission of a completed OTD submission form to the GRC.

2.0 Purpose

The purpose of this standard is to direct the development of a One Time Disposal Submission.

3.0 Scope

This standard is intended to be used by public sector employees responsible for Information Management (IM) within their department, branch or program area who fall under the *Management of Information Act*. It is assumed that the audience for this standard has an understanding of IM principles adequate to enable them to develop the One Time Disposal Submission.

4.0 Required Approach

4.1 Completing the One Time Disposal Submission

The One Time Disposal Submission Template is developed by the OCIO and approved by the *Government Records Committee* as per subsection 5.1(5)(c) of the *Management of Information Act* and is available in *Appendix A*. The following sections provide further

clarification on the various components indicated in the diagram below that will assist you in completing the One Time Disposal Submission template.



Department or Public Body Name
Division or Organizational Unit (if applicable)

One Time Disposal Submission

DEPARTMENTAL/PUBLIC BODY USE									
4.1.1 Number of Boxes/Box Numbers	<table border="1"> <tr> <td>Number of Boxes:</td> <td>Box Numbers (Range):</td> </tr> </table>	Number of Boxes:	Box Numbers (Range):						
Number of Boxes:	Box Numbers (Range):								
	Record Series Title:								
4.1.3 Records Created By Department/ Public Body / Branch/ Division	<table border="1"> <tr> <td>Records Created By Department/Public Body/ Branch /Division:</td> <td>File Date Range: (YYYY-MM to YYYY-MM)</td> </tr> <tr> <td></td> <td>Records Custodian:</td> </tr> <tr> <td></td> <td>Email Address :</td> </tr> <tr> <td></td> <td>Phone No.:</td> </tr> </table>	Records Created By Department/Public Body/ Branch /Division:	File Date Range: (YYYY-MM to YYYY-MM)		Records Custodian:		Email Address :		Phone No.:
Records Created By Department/Public Body/ Branch /Division:	File Date Range: (YYYY-MM to YYYY-MM)								
	Records Custodian:								
	Email Address :								
	Phone No.:								
4.1.6 Department or Public Body ATIPP Coordinator	Departmental or Public Body ATIPP Coordinator:								
	Identification of ATIPP and other Exceptions to Access as Applicable: <ul style="list-style-type: none"> <input type="checkbox"/> Not Applicable <input type="checkbox"/> Section 27 - Cabinet Confidences <input type="checkbox"/> Section 28 - Local public body confidences <input type="checkbox"/> Section 29 - Policy advice or recommendations <input type="checkbox"/> Section 30 - Legal advice <input type="checkbox"/> Section 31 - Disclosure harmful to law enforcement <input type="checkbox"/> Section 32 - Confidential evaluations <input type="checkbox"/> Section 33 - Information from a workplace investigation <input type="checkbox"/> Section 34 - Disclosure harmful to intergovernmental relations or negotiations <input type="checkbox"/> Section 35 - Disclosure harmful to the financial or economic interests of a public body <input type="checkbox"/> Section 36 - Disclosure harmful to conservation <input type="checkbox"/> Section 37 - Disclosure harmful to individual or public safety <input type="checkbox"/> Section 38 - Disclosure harmful to labour relations of a public body as employer <input type="checkbox"/> Section 39 - Disclosure harmful to business interests of a third party <input type="checkbox"/> Section 40 - Disclosure harmful to personal privacy <input type="checkbox"/> Section 41 - Disclosure of House of Assembly service and statutory office records <p>Note: Identify below Federal or Provincial Acts, Regulations or Departmental Public Access Restrictions that are applicable:</p> <p>**Records being transferred to <i>The Rooms Provincial Archives</i> may be made available to the public.</p>								

NOTE - Records management forms are available on the [OCIO website](#) and can be downloaded or completed on-line for printing. Handwritten forms will no longer be accepted.

Please forward completed form to the Government Records Lifecycle Management Unit

OCIO TRIM Number: DOC03551/2010 [V3]

4.1.1 Number of Boxes

A box number is a number assigned by the department or public body. All boxes submitted for disposal should have their own unique number. This number should also be listed on the One Time Disposal Template. For boxes with consecutive numbers, the boxes can be listed as a range of numbers. This information is required by the Government Records Lifecycle

Management Unit and the Government Records Committee. File or record listing may be added in a separate document, which must accompany the Disposal Submission. Refer to [Appendix D](#) and [Appendix E](#).

4.1.2 Record Series Title

The record series title is the name given by the department or public body to the group of records being submitted for disposal.

Record series are a group of records (regardless of format) arranged according to a common filing system or grouped together because they relate to a particular subject or function, result from the same activity, or document the same type of transaction. Record series should be able to be grouped under a common title and should have a common retention and disposal plan. Examples include personnel records, procurement records, and complaint files.

Special media such as photographs, video tapes and maps, etc., must be identified and inventoried separately. Computer disks and microforms must have file listings or indexes provided as well as relevant metadata.

4.1.3 Records Created By Department/Public Body/Branch/Division

Specify the name of the department, public body, branch or division at the time of One Time Disposal submission.

4.1.4 File Date Range

For each submission identify the start and end dates of the record series.

4.1.5 Custodian/Contact Person

This is the person with responsibility for Information Management within the department or public body. This contact will be used by the Government Records Lifecycle Management Unit and The Rooms Provincial Archives staff as the departmental or public body contact.

4.1.6 Departmental or Public Body Access and Privacy Coordinator

Provide the name and contact information for staff responsible for access and privacy within the department or public body.

4.1.7 ATIPP Exceptions

It is important to identify whether the records contain information that may be excluded from access under the [Access to Information and Protection of Privacy Act](#), through either mandatory or discretionary exceptions. This effort may:

- Facilitate processing of ATIPP requests; and
- Impact conditions under which the records may be transferred to The Rooms Provincial Archives.

Identification of potential ATIPP exemptions should be done in consultation with the organization's ATIPP Coordinator.

Other Exemptions such as Provincial Regulations or Acts that prevail over ATIPP should also be listed, as outlined in [Newfoundland and Labrador Regulation 11/07](#).

If the One Time Disposal submission contains records from Federal sources, *PIPEDA* (*Personal Information Protection and Electronic Document Act*) and/or other Federal privacy legislation may apply. The applicable legislation must be identified.

Note: Please be mindful that records being transferred to The Rooms Provincial Archives may be made available to the public.

4.2 Submitting One Time Disposal Submission for Review and Approval

When the One Time Disposal Template has been completed, undertake a final review to ensure that all requirements are being met. The review should include:

- Program manager responsible for records
 - Ensure that all sections are completed correctly
- ATIPP coordinator
 - Verify that potential ATIPP and other exceptions are properly identified
- Legal Services
 - Verify that the total retention period meets legislative requirements
 - Identify potential legal issues
- Finance
 - Confirm that retention periods are appropriate if the One Time Disposal Submission has any financial implications
- Government Records Archivist
 - Ensures that archival appraisal recommendations is complete

Draft copies should be sent to the [Government Records Lifecycle Management Unit](#) and the [Government Records Archivist](#) at The Rooms Provincial Archives for approval before sending the final submission for departmental approval, as further clarifying information may be required.

When the One Time Disposal Submission has been completed, this form may be signed on behalf of a public body, department, board, agency or commission by a person at the Executive level, who is clearly identified, and who has authority to sign for the entity. The Government Records Committee is entitled to rely on the person’s signature as evidence of his/her authority. A *Template Memorandum for Submission of One Time Disposal Submission* is included in [Appendix B](#).

The submission must be made electronically to grlm@gov.nl.ca followed up with the signed *Memorandum for Submission of One Time Disposal Submission*.

The GRC holds monthly meetings and any submission will have to be received by GRLM staff 7 days prior to the next GRC meeting. Please see [Appendix C](#) of this document for further information on the One Time Disposal Submission or direct inquires by telephone to 729-3628 or via e-mail to grlm@gov.nl.ca.

5.0 Definitions and Acronyms

5.1 Definitions

Government Records Committee
Information Management
Office of Primary Responsibility

5.2 Acronyms

ATIPP	Access to Information and Protection of Privacy
GRLM	Government Records Lifecycle Management
GRC	Government Records Committee
IM	Information Management
OCIO	Office of the Chief Information Officer
OPR	Office of Primary Responsibility
OTD	One Time Disposal
RRDS	Records Retention and Disposal Schedule

6.0 Compliance

Mandatory compliance

OCIO Standards are mandatory for users to follow and dictate uniform ways of operating.

7.0 Monitoring and Review

The Information Management Services Branch is responsible for monitoring and reviewing this Standard in accordance with processes set forth by the Corporate and Information Management Services Branch.

8.0 References

Management of Information Act

Information Management and Protection Policy, TBM 2009-335

9.0 Revision History

Date Reviewed	Reviewed By
2015-06-26	Power, Iris (Director, Information Management Services)

Appendix A: One Time Disposal Submission Template



*Department or Public Body Name
Division or Organizational Unit (if applicable)*

One Time Disposal Submission



DEPARTMENTAL/PUBLIC BODY USE	
Number of Boxes:	Box Numbers (Range):
Record Series Title:	
Records Created By Department/Public Body/ Branch /Division:	File Date Range: (YYYY-MM to YYYY-MM)
	Records Custodian:
	Email Address :
Phone No.:	

Departmental or Public Body ATIPP Coordinator:
<p>Identification of ATIPP and other Exceptions to Access as Applicable:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Not Applicable <input type="checkbox"/> Section 27 - Cabinet Confidences <input type="checkbox"/> Section 28 - Local public body confidences <input type="checkbox"/> Section 29 - Policy advice or recommendations <input type="checkbox"/> Section 30 - Legal advice <input type="checkbox"/> Section 31 - Disclosure harmful to law enforcement <input type="checkbox"/> Section 32 - Confidential evaluations <input type="checkbox"/> Section 33 - Information from a workplace investigation <input type="checkbox"/> Section 34 - Disclosure harmful to intergovernmental relations or negotiations <input type="checkbox"/> Section 35 - Disclosure harmful to the financial or economic interests of a public body <input type="checkbox"/> Section 36 - Disclosure harmful to conservation <input type="checkbox"/> Section 37 - Disclosure harmful to individual or public safety <input type="checkbox"/> Section 38 - Disclosure harmful to labour relations of a public body as employer <input type="checkbox"/> Section 39 - Disclosure harmful to business interests of a third party <input type="checkbox"/> Section 40 - Disclosure harmful to personal privacy <input type="checkbox"/> Section 41 - Disclosure of House of Assembly service and statutory office records <p>Note: Identify below Federal or Provincial Acts, Regulations or Departmental Public Access Restrictions that are applicable:</p> <p>**Records being transferred to <i>The Rooms Provincial Archives</i> may be made available to the public.</p>

NOTE - Records management forms are available on the [OCIO website](#) and can be downloaded or completed on-line for printing. Handwritten forms will no longer be accepted.

Please forward completed form to the Government Records Lifecycle Management Unit

OCIO TRIM Number: DOC03551/2010 [V3]

Appendix B: Template Memorandum for One Time Disposal Submission to the Government Records Committee

Memorandum

To: Chair, Government Records Committee

CC: Departmental or Public Body Information Manager, if an ADM or equivalent makes the submission cc the Deputy Minister

From: Deputy Minister, Assistant Deputy Minister or equivalent

Date: 2014-12-04

Re: Request for Approval of One Time Disposal Submission

The (Department or Public Body Name) requests the approval of the Government Records Committee (GRC) of a One Time Disposal Submission

Records Series title:	Description:
-----------------------	--------------

(Responsibility for the development and ongoing operation of Information Management activities has been assigned to (Departmental or Public Body Information Manager Name), the (Position Title). (Departmental or Public Body Access to Information and Protection of Privacy (ATIPP) Coordinator Name and Position Title) is responsible for the implementation of ATIPP for the (Department or Public Body Name). The (Department or Public Body Name) will notify the Government Records Committee in the event that there is a change in resources.

This One Time Disposal Submission has been reviewed for legal (ATIPP), financial, audit and operational requirements.

Please forward inquiries related to the use of the attached One Time Disposal Submission to:

Departmental or Public Body Information Manager Name	Departmental or Public Body ATIPP Coordinator
Mailing Address	Mailing Address
Phone Number	Phone Number
Fax Number	Fax Number
Email Address	Email Address

Sincerely,

Authorized Signing Officer

Authorized Individual's Name
Please Print

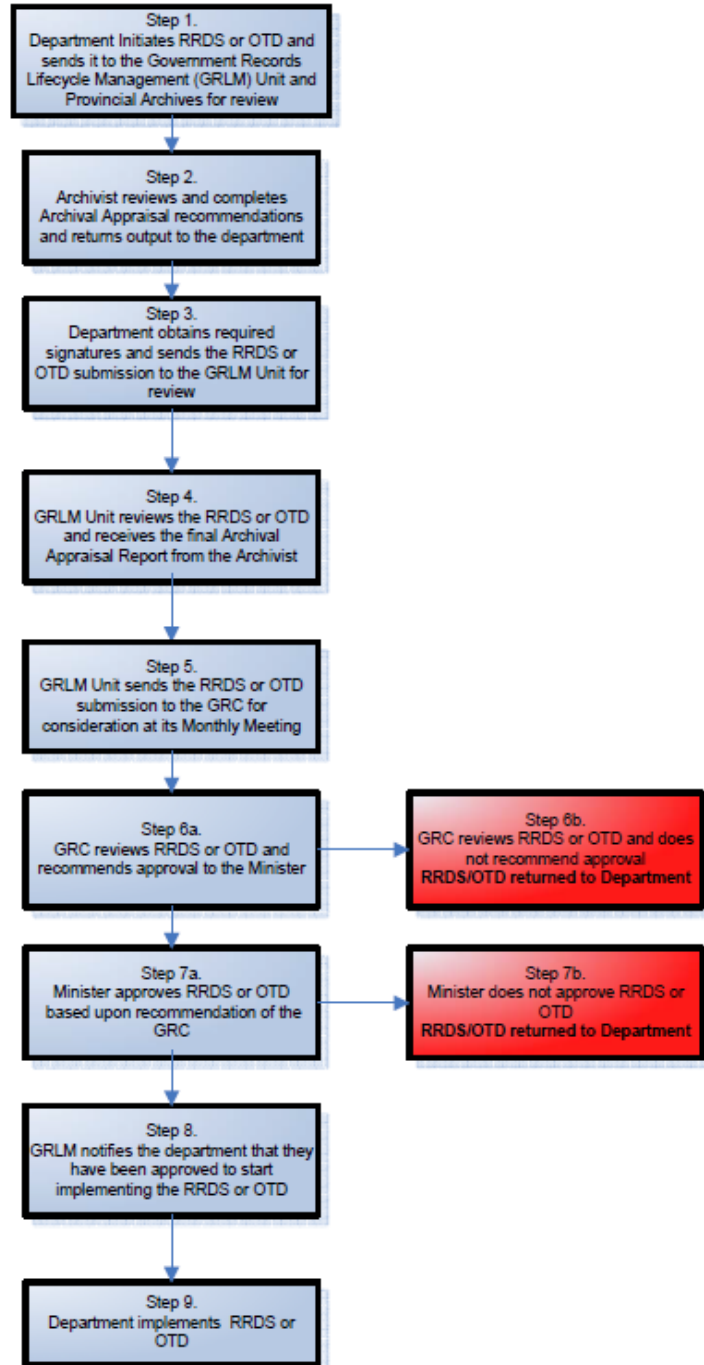
Position

Authorized Signature

Date

Appendix C: Government of Newfoundland and Labrador Records Disposal Process

Government of Newfoundland and Labrador Records Disposal Process
 Use for Records Retention and Disposal Schedules (RRDS) and for One Time Disposal (OTD) Submissions



Appendix D: Records Disposal Submission Checklist



Records Disposal Submission Checklist

Have you fully completed the *One Time Disposal Submission* template?

Have you included a file or record listing?

When developing a file or record listing as part of the *One Time Disposal Submission*, consider the following:

- For each file, identify the earliest and last date of creation using the Government Date Standard (yyyy-mm-dd)
- If file titles are numeric or have alpha numeric titles, please attach copy of file listing index.
- If the files are the files of an employee, list name and employees' position (ie. John Brown, Assistant Director of Technical Services)
- Many departments have developed their own jargon of specialized abbreviations or file and the acronym when it is first listed (ie. Provincial Association of School Tax Authority (PASTA) Committee Minutes 2004).

Have all departmental stake holders (Program Manager, ATIPP Coordinator, Legal Services, and Finance) reviewed the submission to ensure all requirements are met?

Have you sent draft electronic copies of the *One Time Disposal Submission* to the Government Records Lifecycle Management Unit and The Rooms/Provincial Archives for review prior to departmental signoff?

Have you completed the *Memorandum for One Time Disposal Submission to the Government Records Committee* with appropriate signatures?

Have you forwarded the signed original to the Government Records Lifecycle Management Unit for formal submission to the Government Records Committee?

The Submission must include the following:

- *Signed Memorandum for One Time Disposal Submission to the Government Records Committee*
- *Departmental One Time Disposal Submission*
- *Departmental File or Record Listing*

Appendix E: Sample File Listing



Government of Newfoundland and Labrador

FILE LISTING

Department/Public Body:	Branch / Division:
Records Series Title:	
Departmental Box Number:	Schedule Number:

File Date Range (yyyy-mm-dd)		File Title	ATIPP Issues [Y or N]	Litigation issues [Y or N]
From	To			



STANDARD – DEVELOPING RECORDS RETENTION AND DISPOSAL SCHEDULES FOR OPERATIONAL RECORDS

Standard (Definition): OCIO Standards derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. The OCIO standards are mandatory for users to follow and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. Standards are usually defined to support the policies and directives and are supported by Guidelines, where applicable

Issuing Branch	<i>Office of the Chief Information Officer – Corporate and Information Management Services (CIMS)</i>
Date Reviewed	2016-03-05
OCIO TRIM Number	DOC12999/2009[V2]
Authorizing Directive	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
Authorizing Body	Government Records Committee (GRC)
GRC Approval Meeting	2016-004
GRC Approval Number	GRC Meeting 2016-004 (2016-04-12)
Note: Questions related to this Standard should be forwarded to im@gov.nl.ca	

Table of Contents

1.0 Overview 3

2.0 Scope 3

3.0 Records Retention and Disposal Schedule (RRDS) for Operational Records 4

 3.1 Common Requirements..... 4

3.1.1 Office of Primary Responsibility..... 4

3.1.2 Vital Records 5

3.1.3 Access to Information and Protection of Privacy (ATIPP)..... 5

3.1.4 Retention Periods..... 6

3.1.5 Disposition..... 8

 3.2 Requirements Specific to Record Series RRDS 9

3.2.1 Business Unit 9

3.2.2 Business Unit Overview 9

3.2.3 Record Series 10

 3.3 Requirements Specific to Organizational / Divisional RRDS 10

3.3.1 Overview 10

3.3.2 Administrative History 11

3.3.3 Organizational Structure 11

3.3.4 Classification Plan 11

3.3.4.1 Function 12

3.3.4.2 Primary 12

3.3.4.3 Secondary (optional)..... 12

3.3.5 Scope Notes..... 13

4.0 Submitting RRDS for Review and Approval 14

5.0 Implementing the Records Retention and Disposal Schedule..... 15

 5.1 Destruction of Records 15

 5.2 Transfer of Records to Semi-Active Storage..... 15

 5.3 Transfer of Records to the Rooms Provincial Archives 15

6.0 Maintaining the Records Retention and Disposal Schedule 16

7.0 Definitions and Acronyms 16

 7.1 Definitions 16

 7.2 Acronyms 17

8.0 Monitoring and Review 17

9.0 References..... 17

10.0 Revision History 17

11.0 Appendices 18

DEVELOPING RECORDS RETENTION AND DISPOSAL SCHEDULES (RRDS) FOR OPERATIONAL RECORDS STANDARD

1.0 Overview

A records retention and disposal schedule (RRDS or schedule) prescribes records retention periods and disposal plans, can apply to records in any format and authorizes disposal of records in a legal manner. The RRDS can be used for all records in an organization, or for the records of a specific branch or division. It can encompass all types of records within an organization, or may be limited to specific record types or one record series.

The RRDS must include, at a minimum:

- Identification of the Office of Primary Responsibility (OPR). The OPR is the department or public body; or the division or section of a department or public body that created the record in the course of its mandate and that will be responsible for implementing and maintaining the schedule.
- Descriptions of the records covered by the schedule sufficient to allow users to understand which records are included.
- The retention periods of the records in all stages of their lifecycle: from active, through semi-active, to final disposal.
- Legally approved disposal for the records in the schedule – under the *Management of Information Act* and the *Rooms Act*, legal disposal means one of three things: either records are destroyed, transferred to The Rooms Provincial Archives for permanent preservation or permanently retained by the department.
- Identification of Vital Records. These are records which are required to resume business of the organization in the event of catastrophe (e.g., Cabinet records, the documents describing the operations of essential IT systems, and the organization's main financial systems).

The *Management of Information Act* gives authority to the Government Records Committee (GRC) to make recommendations to the Minister to dispose of government records. The RRDS is the recommended disposal authority used for the legal disposal of government records. The purpose of this standard is to describe how to develop an RRDS for Operational Records.

2.0 Scope

This standard is intended to be used by public body employees responsible for information management within their organization. It is assumed that the audience for this Standard has an understanding of IM principles adequate to enable them to develop the RRDS.

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

3.0 Records Retention and Disposal Schedule (RRDS) for Operational Records

The RRDS templates are developed by the OCIO and approved by the GRC as per subsection 5.1(5)(c) of the *Management of Information Act* and are available in the appendices.

There are two standard templates for the creation of retention and disposal schedules for operational records:

1. **Record Series RRDS** – Used when departments or public bodies want to schedule a group of records that relate to a particular function or activity such as one records series or one type of case file. Records will result from the same activity or document the same type of transaction and will have a common retention and disposal plan. Refer to **Appendix A**.
2. **Organizational / Divisional RRDS** – Used when a department or public body wishes to schedule all or most of the records of a program or division of an organization. Some departments or public bodies may organize their records based on a hierarchical classification which may further define primary and secondary levels. Refer to **Appendix B**.

Requirements will vary depending on the type of schedule being developed, whether it is Record Series or Organizational/Divisional RRDS. The following section outlines the requirements needed depending on the type of RRDS being developed:

- Common requirements for both templates
- Requirements specific to the Record Series RRDS
- Requirements specific to the Organizational / Divisional RRDS

3.1 Common Requirements

Regardless of how a department or public body manages their records and which template they choose, the department or public body must identify or determine the following:

- Office of Primary Responsibility
- Vital Records
- ATIPP Exceptions and Other Access Legislation and Issues
- Retention Periods
- Disposition

3.1.1 Office of Primary Responsibility

The Office of Primary Responsibility (OPR) is the organizational unit (branch or division) that maintains the authoritative government record (sometimes called the “original” or “official” record). Organizations are only required to create schedules for the disposal of records for which they are the OPR. Non-OPR records in the custody of an organization may be disposed of as transitory records or copies of convenience without being scheduled when they no longer have any value to the organization.

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

3.1.2 Vital Records

A vital record is defined as one that is indispensable to a mission critical business operation or a record identified as essential for the continuation of an organization during or following a disaster. Such records are required to recreate the organization’s legal and financial status and to support the rights and obligations of employees, customers, shareholders and citizens. Identifying a group of records as vital may mean additional management and security requirements.

3.1.3 Access to Information and Protection of Privacy (ATIPP)

Exceptions and Other Access Legislation and Issues

It is important to identify whether the records contain information that may be excluded from access under the *Access to Information and Protection of Privacy Act*, through either mandatory or discretionary exceptions. This effort may:

- Facilitate processing of ATIPP requests; and
- Impact conditions under which the records may be transferred to The Rooms Provincial Archives. Records being transferred to *The Rooms Provincial Archives* may be made available to the public. Records at the Provincial Archives are mostly available to the public. If records must be closed to the public, it must be identified in the RRDS.
- Requests to access records transferred to The Rooms Provincial Archives that contain Section 30, 34 and 35 exceptions to access issues or have legislation that supersedes ATIPPA will have to be determined by the creating department.

Identification of potential ATIPP exemptions must be done in consultation with the organization’s ATIPP Coordinator. ATIPP exceptions are outlined in the chart that follows and a detailed description and summary is available in **Appendix I**:

Section	Exception
27	Cabinet Confidences
28	Local public body confidences
29	Policy advice or recommendations
30	Legal advice
31	Disclosure harmful to law enforcement
32	Confidential Evaluations
33	Information from a workplace investigation
34	Disclosure harmful to intergovernmental relations negotiations
35	Disclosure harmful to the financial or economic interests of a public body

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

Section	Exception
36	Disclosure harmful to conservation
37	Disclosure harmful to individual or public safety
38	Disclosure harmful to Labour relations interests of public body as employer
39	Disclosure harmful to business interests of a third party
40	Disclosure harmful to personal privacy
41	Disclosure of House of Assembly service and statutory office records
N/A	Not applicable
Other	Other Federal or Provincial Acts or Regulations that prevail over ATIPP, or other Provincial Legislation that affects access.

Other Exemptions:

1. Document other legislation that can affect access to records
2. Provincial Regulations or Acts that prevail over ATIPP and PHIA (Personal Health Information Act) must also be listed, as outlined in Newfoundland and Labrador Regulation 11/07.

If the RRDS contain records from Federal sources, the *Privacy Act* may apply. The applicable legislation must be identified.

Note: Records being transferred to *The Rooms Corporation, Provincial Archives Division* may be made available to the public. If there are any issues with records being made available to the public, it must be identified in the RRDS as it can affect the archival value.

3.1.4 Retention Periods

A retention period represents the period of time in which a record must be kept or “retained”. Retention periods must be identified for records in all stages of their lifecycle: from active, through semi-active, to final disposition.

Acronym	Definition
ACT	Active: Identifies how long the records will be stored onsite to support operational requirements. Expressed using the acronyms CY, FY, ED or S/O plus the total number of years.
SA	Semi-Active: Identifies how long records are stored in semi active storage to fulfill operational and legal requirements for retention. Typically expressed as a number of years. CY or FY
CY	Calendar Year: The retention period is applied at the end of the calendar year, December 31st (e.g., CY+2 means that records will be retained for the current calendar year plus an additional 2 years for a total of 3 years).

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

Acronym	Definition
FY	Fiscal Year: The retention period is applied at the end of the fiscal year, March 31st (e.g., FY+2 means that records will be retained for the current fiscal year plus an additional 2 years for a total of 3 years).
ED	Event Date: The retention period is applied when an event has occurred (e.g. ED+2 means that records will be retained for 2 years after the end of a project). Event date should be identified in RRDS and should clarify if year is CY or FY.
S/O	Superseded/Obsolete: The retention period will apply only when it has been determined that the records are either superseded or obsolete (e.g., a policy has been updated so the existing policy is now S/O).
N/A	Not applicable: This element of the RRDS does not apply.

Active Stage

Active Storage identifies how long records need to be easily accessible to support ongoing operations. This usually means keeping them onsite in the office or within the building of immediate use.

When determining how long records need to be retained in active storage, the best source is the employees who actually use the records.

There are two options for assigning the time period for the active stage in the records lifecycle:

- 1) Time-based retention
 - Easy to implement because records are simply boxed up and transferred at the end of the calendar or fiscal year
 - Expressed as either Calendar Year (CY) + # of Years or Fiscal Year (FY) + # of Years
- 2) Event-based
 - Used when the disposal of records is dependent on something happening such as the resolution of a claim, completion of a project, etc.
 - More effort to implement because it requires tracking the retention events in order to implement the schedule when they occur
 - Expressed as either Event Date (ED) + # of Years or Superseded/Obsolete (S/O)+ # of Years either CY or FY.
 - Identify what the Event Date symbolizes (i.e ED = File Closed). This will ensure individuals in the future will understand what the event date is and can apply the appropriate retention.

Semi-Active Stage

Semi-active storage identifies how long records need to be retained by the department or public body (usually off-site) to meet both operational and legal retention requirements. When completing this section, the best source for this information is:

- Employees who use the records
- Subject matter experts

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

- RRDS used by other jurisdictions may be helpful in identifying industry standards and any applicable federal government requirements
- Legislation
- Legal Agreement
- Legal Counsel

Final Disposition Stage

Final disposition refers to what happens to the records when the department or public body has fulfilled all of its operational needs and legal obligations to retain its records. The disposal methods will be explained in the section that follows.

3.1.5 Disposition

The *Rooms Act*, gives authority to the Provincial Archivist to decide what is archival. The Government Records Archivist (GRA), through The Rooms Provincial Archives, will conduct an archival appraisal to help determine the appropriate disposition. This appraisal will identify which records have enduring value for permanent preservation and what records are non-archival and can be destroyed upon completion of the retention period. The GRA must be notified at the beginning of the RRDS development process, after the initial draft is created.

Once notified that a RRDS is being developed the GRA will:

- Estimate how long the archival appraisal will take based on the scope of the RRDS
- Refer creating public body to OCIO IM Advisory Services.
- Ensure that resources are available to review RRDS based on the proposed timeline
- Identify whether other staff from The Rooms Provincial Archives will need to be involved in appraisal. This will be based on information formats and the scope of the RRDS
- Undertake necessary research related to the RRDS including:
 - Organizational history
 - Similar retention schedules from other jurisdictions
 - Contacting departmental staff to gather additional information.

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

Dispositions are outlined in the chart that follows:

Acronym	Definition
D	Destruction: Records will be securely destroyed when retention requirements have been met.
AR	Archival Retention: All records in a particular record series will be retained by The Rooms Provincial Archives when the department or public body has fulfilled operational and legal requirements to maintain the records.
SR	Selective Retention: A portion of the records will be retained by The Rooms Provincial Archives when the department or public body has fulfilled operational and legal requirements to maintain the records. In the case of Selective Retention (SR), the Government Records Archivist will determine the parameters for these records (e.g., projects with a dollar value above XX or claims that result in a financial settlement).
PRD	Permanent Retention by Department: Records that are required to be kept indefinitely by a public body because of a statutory/regulatory requirement or the physical format of the records or a specific/enduring business need. In the case of Permanent Retention by Department (PRD), the Government Records Archivist will not accession these records and they will remain under the custody and control of the department.
N/A	Not applicable: This element of the RRDS does not apply.

3.2 Requirements Specific to Record Series RRDS

The *Record Series RRDS Template* is available in **Appendix A**. In addition to the common requirements described in section 3.1, a department or public body must identify, describe or determine the following:

- Business Unit
- Business Unit Overview
- Records Series

3.2.1 Business Unit

Specify the name of the department or business unit at the time of Retention Schedule submission.

3.2.2 Business Unit Overview

Provide a high level overview of the business unit capturing the mandate of the unit. This can typically be found in documents such as an organization’s Business Plan and Annual Report under departmental mandate.

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

3.2.3 Record Series

Identify the record series being submitted for scheduling.

Record series are a group of records (regardless of format) arranged according to a common filing system or grouped together because they relate to a particular subject or function, result from the same activity, or document the same type of transaction. Record series should be grouped under a common title and have a common retention and disposal plan.

Examples include personnel records, procurement records, and complaint files.

Completing the description may require interviews with subject matter experts and program specialists within the organization to verify that all descriptive information has been identified and is accurate. A sample list of interview questions is included in **Appendix C**.

At a minimum the following information must be captured when describing the record series:

- What information the record series contains.
- The functions of the record.
- The creator and users of the records and how they are used.
- The record format (i.e. electronic, paper, etc.).
- The legislation that affects the records

3.3 Requirements Specific to Organizational / Divisional RRDS

A department or public body who manages their records according to their mandated function or activity would schedule their records using the *Organizational/ Divisional RRDS Template*, see **Appendix B**.

Some departments or public bodies may organize their records based on a hierarchical classification which may further define primary and secondary levels. Secondary levels are not mandatory but must be identified if they are part of your classification scheme.

In addition to the common requirements described in section 3.1, the following information must be defined:

- Overview
- History
- Classification Hierarchical Structure
- Scope Notes
- Arrangement and Classification Numbers

3.3.1 Overview

Provide a high level overview of the Organization or division capturing the mandate of the unit. This can typically be found in documents such as an organization's Business Plan and Annual Report under departmental mandate.

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

3.3.2 Administrative History

Provide a high level overview of when the department was established and any relevant organizational changes of importance.

3.3.3 Organizational Structure

Provide the current organizational structure that identifies roles/positions only. Exclude employee names from the diagram.

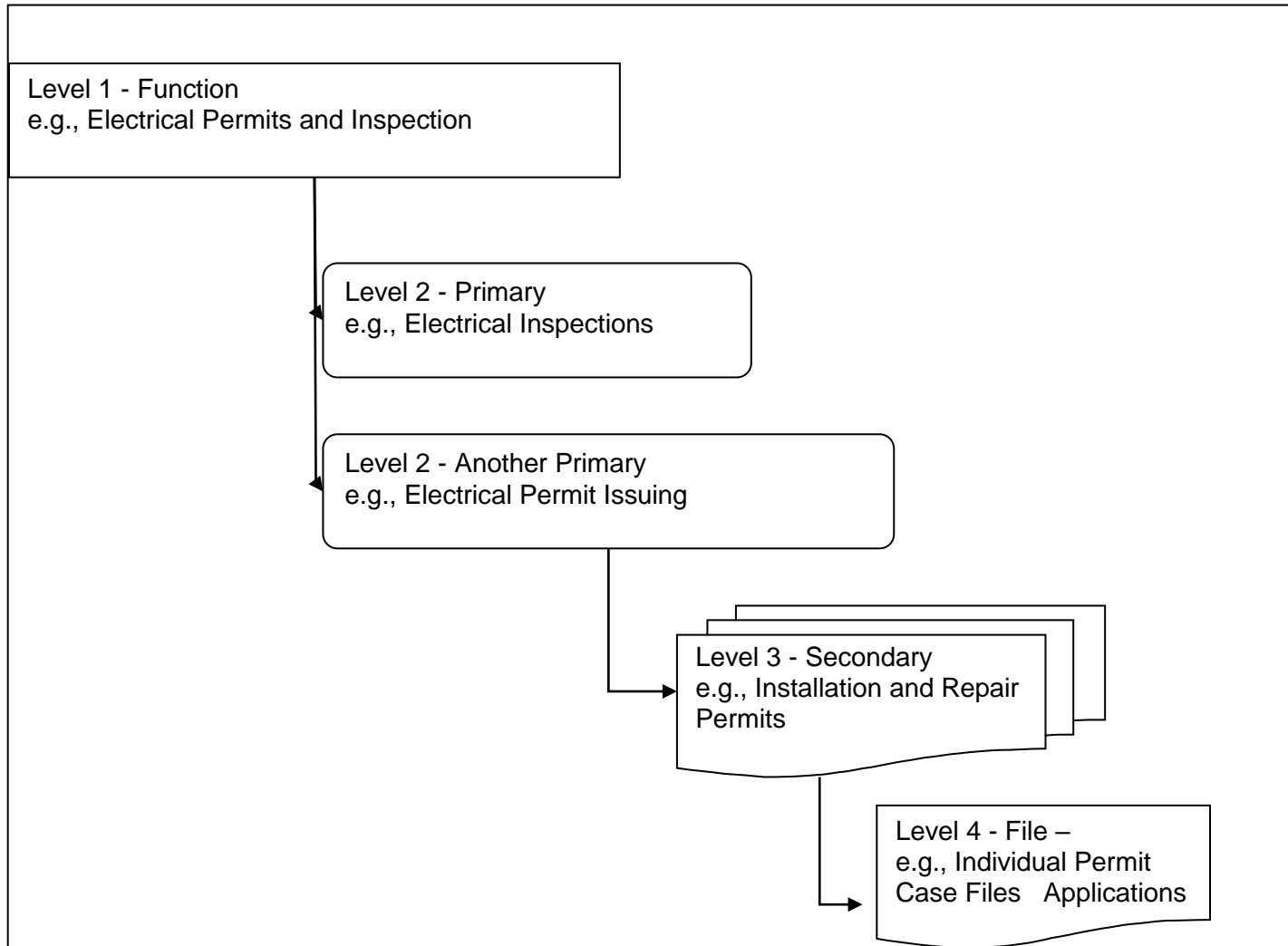
3.3.4 Classification Plan

A hierarchical classification plan organizes records in a fashion that makes it easier to manage them through their life-cycle. Classification plans for operational records capture business functions relevant to a department, rather than subjects, the labels used to describe each level of the hierarchy will be different.

The hierarchical structure of the classification plan is three-tiered, going from the general to the specific, followed by individual containers or folders at the “file level” as the fourth level shown on the following page. The number of levels used will vary from organization to organization and are generally referred to as the following, which are explained below in more detail:

- Function
- Primary
- Secondary

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records



3.3.5 Function

The function is at the highest level on the classification plan and clusters together the next level of sub-functions and activities relating to that function. It represents a grouping of primary activities required to meet a particular mandate. For example, *Electrical Inspection* and *Electrical Permit Issuing* are sub-functions of *Electrical Permits and Inspection* and therefore are identified as separate primaries grouped under this function.

3.3.6 Primary

The primary is the next level and represents a grouping of secondary functions and activities that support the function it is attached to at the higher level. For example, the activities of receiving permit applications, review and approval by the Chief Electrical Inspector and the issuing of permits for electrical work in installation and repairs and electrical maintenance that support the primary *Electrical Permit Issuing* would form secondaries under this primary.

3.3.7 Secondary (optional)

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

The secondary is the next level and represents groupings of activities performed and some record series that support the higher level. We recommend using two types of secondaries: common and function specific secondaries. Common secondaries are those activities and record series commonly listed under each primary (e.g., *Working Groups*). Function specific secondaries are specialized types of activities and records series that are unique to that primary (e.g., *Installation and Repair Permits* under the Primary called *Electrical Permit Issuing*). See C-RIMS for common secondaries.

3.3.8 Scope Notes

Scope notes provide users with enough information to assist them in making the correct decision for identifying and capturing their records. This information is also important when developing an RRDS. Descriptions must be consistent in the organization of information being communicated. Each level refers to the next level in that it describes the groupings at the next lower level.

The description must contain a statement that includes the following types of information: 1) a definition of the function, primary or secondary; 2) a summary of the primaries or secondaries or records series beneath that level in the hierarchy; and 3) the types of information and records found in that specific classification. As you descend the level, additional information may be included (e.g., specific filing arrangements or a cross-reference to another classification).

Scope Notes Example
<p>Level 1 – Function Scope Notes Electrical Permits and Inspection The Electrical Permits and Inspection function provides a means to ensure public safety through regulation of electrical work being carried out by certified electricians and registered contractors. The Chief Electrical Inspector reviews applications, approves and issues electrical permits allowing electrical work to be carried out and conducts inspections of contractors' electrical work as defined in <i>the Public Safety Act</i>, snl1996 c.p-41.01 and Electrical Regulations nlr120/96.</p>
<p>Level 2 - Primary Scope Notes Electrical Permit Issuing Chief Electrical Inspector review and approval of permit applications that must be issued before installation or repair of any electrical equipment commences. The primary includes the issuance of two different permits: one for electrical installation and repair and the other for electrical maintenance.</p>
<p>Level 3 - Secondary Scope Notes Installation and Repair Permits Case Files Use for application submissions for electrical installation and repair permits for both single and non-single dwellings. Information includes permit applications, specifications of electrical work, building plans, approvals, permits, declines, and appeals. Arranged by applicant name and permit number.</p>

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

4.0 Submitting RRDS for Review and Approval

When the RRDS template has been completed, undertake a final review to ensure that all requirements are being met. The review should include discussion with the following individuals:

- Program manager responsible for records
- Government Records Archivist
 - Ensure that archival appraisal is complete
- ATIPP coordinator
 - Verify that potential ATIPP and other exceptions are identified properly
- Legal Services
 - Verify that total retention period meets legislative requirements
 - Identify potential legal issues
- Finance
 - Confirm that retention periods are appropriate if the RRDS contains any financial implications

Once the RRDS has been approved by the Department, the Deputy Minister, Assistant Deputy Minister or equivalent must review the final RRDS and submit a request to the Government Records Committee (GRC). Refer to **Appendix E** for the *GRC Submission Process* flow diagram. In the case of boards, authorization is required from the Chair or the Chief Executive Officer (CEO). A *Template Memorandum for Submission of Records Retention and Disposal Schedule to the Government Records Committee* is included in **Appendix D**.

Schedules must be submitted electronically to grlm@gov.nl.ca followed up with the original signed Memorandum for Submission of Records Retention and Disposal Schedule to the Government Records Committee.

The GRC meets monthly, meeting the second Tuesday of every month. For further information on the RRDS submission and approval process telephone 729-3628 or e-mail grlm@gov.nl.ca

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

5.0 Implementing the Records Retention and Disposal Schedule

The department or public body is responsible for the ongoing implementation of approved records retention and disposal schedules in a consistent and timely manner as a course of regular business. This includes:

- secure destruction of records
- transfer of records to semi-active storage
- transfer of records to The Rooms Provincial Archives
- keep listings of records destroyed

5.1 Destruction of Records

For records that have a disposition of destroy refer to the guideline for [Disposal of Records](#). The department or public body must retain the certificate of destruction to show that destruction of records had legal authority. *Must also retain lists of records destroyed.*

5.2 Transfer of Records to Semi-Active Storage

Semi-active storage includes transfer of records to the Provincial Records Centre (PRC), a commercial storage facility, or a storage facility owned and operated by the organization. Records storage is available to those public bodies whose information technology services are provided by the OCIO. The PRC provides secure storage for the following classes of semi-active government records:

- Vital Records that are identified as either indispensable to a mission critical business operation or essential for the continuation of an organization during or following a disaster.
- Records for which the legal or operational needs of the department or public body dictate that custody and/or control of the information must remain within government.
- Records which, due to their enduring value or historical significance, are to be transferred to The Rooms Provincial Archives Division when no longer required by the department or public body.
- Records which have longer than usual semi-active retention periods may be considered, to lessen the burden of storage costs on departments and public bodies.
- Records must have an approved Records Retention and Disposal Schedule (RRDS).

Refer to IM Advisories for [Preparing Paper Records for Offsite Storage](#) and [Transferring Records to the Provincial Records Centre](#).

5.3 Transfer of Records to the Rooms Provincial Archives

The Rooms Provincial Archives will accept records that have been pre-approved by the Government Records Committee (GRC) as having the disposition of Archival or Selective Retention on the RRDS. Consult with the [Government Records Archivist](#) on how to transfer records to The Rooms Provincial Archives.

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

Refer to IM Advisories for *Preparing Paper Records for Offsite Storage* and *Transferring Records to the Rooms Provincial Archives*.

Note: ATIPPA restrictions and other restrictions to access must be identified at the file level.

6.0 Maintaining the Records Retention and Disposal Schedule

The retention and disposal schedule must be reviewed on a regular basis to identify whether amendments are needed, change of ownership is required, or validity of RRDS has changed. Should any of these occur notify the GRC.

Refer to **Appendices F, G and H** to assist in submitting an amendment to an RRDS.

7.0 Definitions and Acronyms

7.1 Definitions

<p><i>Government Records Committee</i></p>	<p>The Government Records Committee (GRC) is the official body that is mandated to: (1) Review and revise schedules for the retention, disposal, destruction or transfer of government records;(2) Make recommendations to the minister respecting public records to be forwarded to The Rooms, Provincial Archives; (3) Authorize disposal and destruction standards and guidelines for the lawful disposal and destruction of public records; and (4) Make recommendations to the minister regarding the removal, disposal and destruction of records (source: <i>Management of Information Act SNL2005 c.M-1.01</i>).</p>
<p><i>Office of Primary Responsibility</i></p>	<p>The Office of Primary Responsibility (OPR) is the organization and/or position within an organization that is responsible for maintaining the integrity of a record (source: Corporate Records and Information Management Standard (C-RIMS)).</p>
<p><i>Record Series</i></p>	<p>Record series are a group of records (regardless of format) arranged according to a common filing system or grouped together because they relate to a particular subject or function; result from the same activity or document the same type of transaction. Record series should be able to be grouped under a common title and should have a common retention and disposal plan.</p>

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

<i>Vital Records</i>	A vital record is defined as one that is indispensable to a mission critical business operation or a record identified as essential for the continuation of an organization during or following a disaster. Such records are required to recreate the organizations legal and financial status and to support the rights and obligations of employees, customers, shareholders and citizens (source: Making the Transition from Paper to Electronic, David O. Stephens, ARMA International, 2007).
-----------------------------	--

7.2 Acronyms

ATIPP	Access to Information and Protection of Privacy
GRC	Government Records Committee
OCIO	Office of the Chief Information Officer
OPR	Office of Primary Responsibility
RRDS	Records Retention and Disposal Schedule

8.0 Monitoring and Review

The IM Branch is responsible for monitoring and reviewing this Standard and all other Information Management and Protection policies, directives, standards and guidelines issued by the OCIO, in accordance with processes set forth by the Corporate Operations and Client Services Branch.

9.0 References

*Management of Information Act
Rooms Act*

Information Management and Protection Policy, TBM 2009-335
 Classification Plan Development for Operational Records Guideline, DOC03307/2011
 Corporate Records and Information Standard, DOC01106/2008*

10.0 Revision History

Version	Date Reviewed	Reviewed By
01	2009-10-06	Porter, Kim – Coordinator, GRLM GRC Meeting 2009-08
02	2014-06-25	Porter, Kim – Coordinator, GRLM GRC Meeting 2009-08

Standard – Developing Records Retention and Disposal Schedules (RRDS) for Operational Records

11.0 Appendices

Appendix A:	Record Series RRDS Template
Appendix B:	Organizational / Divisional RRDS Template
Appendix C:	Sample List of Questions for RRDS Interviews
Appendix D:	Template Memorandum for Submissions of Records Retention and Disposal Schedule to the Government Records Committee
Appendix E:	GRC Submission Process
Appendix F:	Maintaining and Amending Records Retention and Disposal Schedules
Appendix G:	Memorandum for Amending Records Retention and Disposal Schedules
Appendix H:	RRDS Summary of Changes
Appendix I:	Summary of ATIPP Exceptions

Appendices are available online on OCIO's [website](#).



STANDARD – CORPORATE RECORDS INFORMATION MANAGEMENT STANDARD

Standard (Definition): OCIO Standards derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. The OCIO standards are mandatory for users to follow and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. Standards are usually defined to support the policies and directives and are supported by Guidelines, where applicable

Issuing Branch	<i>Office of the Chief Information Officer – Corporate and Information Management Services (CIMS)</i>
Date Reviewed	2016
OCIO TRIM Number	DOC01106/2008[V2]
Authorizing Directive	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
Authorizing Body	Government Records Committee (GRC)
GRC Approval Meeting	2016-004
GRC Approval Number	GRC Meeting 2016-004 (2016-04-12)

Note: Questions related to this Standard should be forwarded to im@gov.nl.ca

Table of Contents

1.0 Overview 5

2.0 Purpose..... 5

3.0 Scope 5

4.0 Background..... 5

5.0 C-RIMS Classification Plan 5

 5.1 Common Secondaries..... 7

 5.2 Special Notes on the Records of Committees 9

 5.3 Special Note on Commissions of Inquiry..... 10

 5.4 Office of Primary Responsibility (OPR) 10

5.4.1 Government OPR 10

5.4.2 Department OPR..... 10

5.4.3 Non-OPR 10

 5.5 Numeric Arrangement and Title Conventions 11

 5.6 C-RIMS Corporate Functions and Primaries..... 11

6.0 C-RIMS Retention and Diposal Schedule 13

 6.1 EXECUTIVE FUNCTIONS – 01 13

6.1.1 Department Briefing Notes - 01 13

6.1.2 Executive Council Briefing Notes – 02 13

6.1.3 Briefing Books – 03..... 14

6.1.4 Transition Briefing Books – 04 14

6.1.5 Cabinet Papers – 05 15

 6.2 COMMUNICATION MANAGEMENT – 02 15

6.2.1 Media Relations - 01..... 16

6.2.2 Advertising - 02 16

6.2.3 Internal Communication - 03..... 17

6.2.4 Communication Plan – 04 17

 6.3 FINANCIAL MANAGEMENT – 03..... 18

6.3.1 Accounts Payable - 01 18

6.3.2 Accounts Receivable - 02..... 19

6.3.3 Banking - 03 20

6.3.4 Budget Planning and Monitoring - 04 20

6.3.5 Employee Pay and Compensation – 05 22

6.3.6 Procurement - 06..... 23

6.3.7 General Ledger - 07..... 25

6.3.8 Financial Delegation - 08 26

 6.4 HUMAN RESOURCES MANAGEMENT – 04..... 27

Standard – Corporate Records Information Management Standard (C-RIMS)

- 6.4.1 **Employee Relations – 01** 27
- 6.4.2 **Integrated Disability Management – 02**..... 28
- 6.4.3 **Organizational Development – 03**..... 30
- 6.4.4 **Personal File Management – 04**..... 31
- 6.4.5 **Position Establishment, Classification and Compensation – 05** 31
- 6.4.6 **Staffing and Recruitment – 06** 32
- 6.4.7 **Strategic Human Resource Planning - 07**..... 33
- 6.5 **ASSET MANAGEMENT – 05**..... 34
 - 6.5.1 **Asset Inventory - 01** 34
 - 6.5.2 **Asset Maintenance – 02**..... 35
 - 6.5.3 **Asset Disposal - 03** 35
- 6.6 **FLEET MANAGEMENT – 06** 36
 - 6.6.1 **Vehicular Accidents – 01**..... 36
 - 6.6.2 **Fleet Maintenance – 02** 37
 - 6.6.3 **Fleet Disposal - 03**..... 37
- 6.7 **REAL PROPERTY MANAGEMENT – 07** 38
 - 6.7.1 **Design and Construction – 01** 38
 - 6.7.2 **Inventory – 02** 39
 - 6.7.3 **Use and Management – 03** 39
 - 6.7.4 **Disposal - 04** 40
- 6.8 **INFORMATION MANAGEMENT AND PROTECTION – 08** 40
 - 6.8.1 **Classification and Retention – 01**..... 41
 - 6.8.2 **Records Inventory – 02**..... 41
 - 6.8.3 **Information Protection – 03**..... 42
 - 6.8.4 **Information Protection Breaches – 04** 42
 - 6.8.5 **Record Disposal - 05**..... 43
- 6.9 **INFORMATION TECHNOLOGY – 09** 44
 - 6.9.1 **IT Service Support – 01** 44
 - 6.9.2 **System Development and Maintenance – 02** 45
- 6.10 **SAFETY AND SECURITY MANAGEMENT – 10**..... 45
 - 6.10.1 **Emergency Planning – 01**..... 45
 - 6.10.2 **Disaster Recovery – 02**..... 46
 - 6.10.3 **Physical Security – 03** 46
 - 6.10.4 **Personnel Security - 04** 47
- 6.11 **COMPLIANCE MANAGEMENT – 11** 48
 - 6.11.1 **ATIPP Request Management – 01** 48

Standard – Corporate Records Information Management Standard (C-RIMS)

6.11.2	Red Tape Reduction - 02	48
7.0	Roles and Responsibilities	49
8.0	Definitions and Acronyms	49
8.1	Definitions	49
8.2	Acronyms	50
9.0	Compliance and Enforcement.....	50
10.0	Monitoring and Review.....	50
11.0	References.....	51
12.0	Revision History	51
13.0	Appendicies.....	51

1.0 Overview

C-RIMS is a standard classification plan designed to replace IMSAR and offer a standard nomenclature and classification rules for common corporate records in all departments. Since the release of IMSAR in 1999, the GNL has seen a dramatic increase in the ways and means of creating, managing, storing and disposing of records in a hybrid environment in which both paper and electronic records are used. C-RIMS can be used to assist in the management of these paper and/or electronic records.

2.0 Purpose

The purpose of this standard is to capture the common functions of the GNL departments and provide a tool for the classification of records, regardless of format, which are created in the performance of those functions.

3.0 Scope

The scope of the application of C-RIMS is all departments within the Government of Newfoundland and Labrador. Other public bodies may adopt this standard if it is deemed by them to suit their needs. The primary audience for this document is Information Management (IM) staff within the GNL.

4.0 Background

In March 1999, the Information Management System for Administrative Records (IMSAR) was released as a joint initiative of the Provincial Archives of Newfoundland and Labrador and the Records and Information Management Committee of the Government of Newfoundland and Labrador. As an integrated records classification system and retention and disposal schedule, it provided the Government of Newfoundland and Labrador (GNL) with a standard to apply to its organization, retention, and disposal of corporate records. In the GNL, the terms records management and information management are used interchangeably.

In February 2009, the initial release of C-RIMS updated terminology and, where appropriate, retention and disposition for common records found throughout the GNL. As well, C-RIMS captures changes in role and mandate of various departments throughout the GNL. Created by the Information Management Branch (IMB) of the Office of the Chief Information Officer (OCIO) in conjunction with the Provincial Archives and the Information Management Standards Board (IMSB), C-RIMS is a key component of any departmental information management program

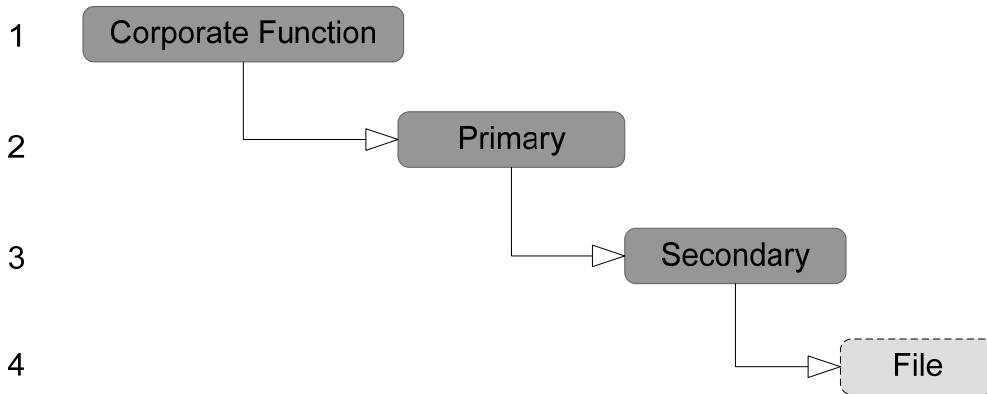
5.0 C-RIMS Classification Plan

C-RIMS is a hierarchical classification plan that organizes records in a fashion that makes it easier to manage them through their life cycle. Like many classification plans, C-RIMS supplies rules on how to categorize records in a meaningful and consistent manner. The approach taken with C-RIMS is somewhat different than traditional records management classification plans. It focuses more towards capturing common functions found in a department, rather than common

Standard – Corporate Records Information Management Standard (C-RIMS)

subjects, the labels used to describe each level of the hierarchy will be different. The following table details each level within the classification.

Levels



Classification Level	Title	Description
1	Corporate Function	The highest level on the classification plan, the Corporate Function is a cluster of primary levels that are similar in nature. It represents a grouping of activities required to meet a particular mandate.
2	Primary	The primary level represents a grouping of secondary level functions. At this point, the Office of Primary Responsibility is designated.
3	Secondary	The secondary level is a mixture of common record types and activities performed. Secondaries are broken into common and function specific categories. Common secondaries are found in all primaries (e.g. policy); however function specific secondaries are specialized types of records and/ or activities that are unique to that primary (e.g. Building Plans under the Primary called Construction).
4	File	The lowest level of the classification plan, the File is where the document (or information object) exists.

5.1 Common Secondaries

Secondary numbers 00 to 40 are reserved for secondaries which are common across all Primaries in C-RIMS. Gaps have been left in numbering for the addition of another Common Secondaries in the future.

COMMON SECONDARIES			
No.	Common Secondaries	ACT	DIS
01	<p>Policy, Orders, Directives, Standards and Guidelines Used to manage and store all records that provide the user with formal direction. These records may have an official number affixed to it by the originating OPR and this number is to be added to the naming convention, as applicable. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Type of document – Title – Approval # - Year Format • Version and/or Revision Control 	SO	D
02	<p>Legislation <i>RECIDED</i> Rationale: <i>Legislation is publicly available on the internet; any work being done by non-OPRs would be covered under common secondaries 10 and 11.</i></p>	N/A	N/A
03	<p>Agreements and Contracts Used to manage and store all records associated with relevant agreements or contracts, including standing offers, MOU's etc. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Document Type – Title – Year format • Version Control and/or Revision Control 	SO	D
04	<p>Associations and Conferences <i>RECIDED</i> Rationale: <i>Associations and Conferences are highly improbable for Non-OPRS.</i></p>	N/A	N/A
05	<p>Complaints Used to manage and store all records associated with work involved in the receiving of a complaint against the particular function. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Complaint – Complainant (Last Name, First Name) – Year Format 	SO	D
06	<p>Planning Used to manage and store all planning type records associated with the function: strategic planning, budgetary planning, etc. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Record Type – Year Format • Version Control and/or Revision Control 	SO	D
07	<p>Orders and Directives <i>Covered under common secondary # 01 Policy, Orders, Directives, Standards and Guidelines</i></p>	N/A	N/A

Standard – Corporate Records Information Management Standard (C-RIMS)

COMMON SECONDARIES			
No.	Common Secondaries	ACT	DIS
08	<p>Reports Used to manage and store all reports received regarding the particular function. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Name of Report • Version Control and/or Revision Control 	SO	D
09	<p>Forms and Templates Used to manage and store all forms or templates associated with the function. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Name of Form • Version Control and/or Revision Control 	SO	D
10	<p>Interdepartmental Committees Used to manage and store all records associated with an Inter-Departmental Committee in which the membership is not in a Chairperson or secretary role. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Type of Committee - Name of Committee 	SO	D
11	<p>Departmental Standing Committee /Steering Committee / Ad-Hoc Departmental Committee or Working Group Used to manage and store all records associated with an Interdepartmental Committee or Working Group that the membership is not the Chairperson or secretary role. If the primary role is one of these then these records must be treated as operational and assigned an individual RRDS. Implementation:</p> <ul style="list-style-type: none"> • Naming Convention = Type of Committee – Name of Committee 	SO	D
12	<p>Steering Committee <i>Covered under common secondary # 11 Departmental Standing Committee /Steering Committee / Ad-Hoc Departmental Committee or Working Group</i></p>	N/A	N/A
13	<p>Ad-Hoc Departmental Committee <i>Covered under common secondary # 11 Departmental Standing Committee /Steering Committee / Ad-Hoc Departmental Committee or Working Group</i></p>	N/A	N/A
14	<p>Working Group <i>Covered under common secondary # 11 Departmental Standing Committee /Steering Committee / Ad-Hoc Departmental Committee or Working Group</i></p>	N/A	N/A

5.2 Special Notes on the Records of Committees

Governance occurs at multiple levels within the GNL. The highest level of governance occurs within the Cabinet process; however governance also includes the oversight of projects; decision-making within departments; and interaction with internal and external stakeholders who have an influence on decision-making (e.g., industry advisory committees or councils and cross departmental committees). With regards to the retention of Sub-Committee records, these records inherit the retention schedule(s) of the overseeing Committee.

Type of Committee	Office of Primary Responsibility (OPR)	Comments
Cabinet Committee	Cabinet Secretariat	As per Section 5.4 (1) <i>Management of Information Act</i> the use and management of Cabinet records is governed by Cabinet Secretariat.
Inter-departmental Committee	The lead Department chairing the committee should take responsibility for retaining the records of the committee.	Copies distributed to members of an inter-departmental committee can and should be securely disposed of in a timely manner when no longer required.
Departmental Standing Committee (e.g., Executive Committee)	Committee chair should be responsible for managing the records of the committee.	Committees of this nature meet regularly to deal with routine departmental matters.
Steering Committee (e.g., Project Steering Committee)	Committee chair should be responsible for managing the records of the committee.	Records of a project Steering Committee are the responsibility of the Project Manager, who should take the necessary measures to ensure they are properly managed.
Ad Hoc Departmental Committee (e.g., Committee established to address a specific topic or issue)	Committee chair should be responsible for managing the records of the committee.	According to the <i>Excellence in Governance</i> handbook (2005) by Cabinet Secretariat, an Ad Hoc Committee is created on “occasions when issues of a time-limited and critical-nature necessitate the establishment of ad hoc committees. Once the time limit has been reached and the report submitted members should understand that the role of the committee is completed and it is duly dissolved.”
Working Group	The Working Group chair should be responsible for managing the records of the group.	Although Working Groups may seem similar to Ad Hoc Committees, they are more transient in nature and usually have a narrow scope of work to accomplish.

5.3 Special Note on Commissions of Inquiry

Any commission that is created under powers of the *Public Inquires Act(2006)* has to comply with Section 28 of the Act which states “The Lieutenant-Governor in Council shall adopt policies and procedures for the preservation of the records of a commission or inquiry and shall ensure that confidentiality is preserved for information that is confidential or privileged.” Note, a Commission that bears in its title “Royal” or any other variant (i.e. Review, Investigation) has no bearing on its powers. Although such terms may emphasize a level of importance, they are all equal under the *Public Inquires Act, 2006*.

5.4 Office of Primary Responsibility (OPR)

A key component to any records and information management classification and retention system is knowing the OPR. The OPR is the organization and/or position within an organization that is responsible for maintaining the integrity of a particular record type. By knowing the OPR, it increases the certainty that all records in a records series are collected and managed as per the OPR requirements to ensure complete records and the consistent, secure disposition of additional records.

C-RIMS has two approaches to OPRs: at the Government-wide level, and at the departmental level.

Note: In most instances the Government OPR and the Department OPR will be the same entity.

5.4.1 Government OPR

The Government OPR is the department that is responsible for keeping a master record on behalf of the government. The Government OPR has a legislative or executive mandate for the record series. It is the Government OPR that creates the policy, directives, or legal requirements for the record series on behalf of Government.

5.4.2 Department OPR

Department OPR is the department that is responsible for keeping the master record of all records received or created in a record series. It is the Department OPR that is mandated with the administration of the function on behalf of Government and is the main point of contact for other Departments in the administration of the particular function.

5.4.3 Non-OPR

In order to facilitate the need to reduce duplication and ensure proper disposal, C-RIMS has designated the retention and disposition schedules for each secondary level for all Non-OPR parties. This will reinforce efforts to maintain the integrity of a record within the OPR as well as offer clear direction for Non-OPR parties.

5.5 Numeric Arrangement and Title Conventions

The following is a list of guidelines that address numeric arrangement and title conventions with C-RIMS:

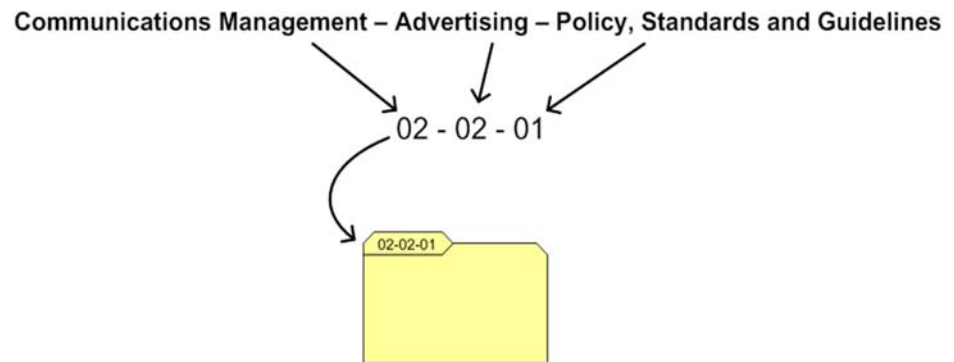
Only use dashes (-) between numbers and/or the title of each level. Avoid using periods (.), slashes (/) or any other common separators.

Numeric arrangement should be presented in which the highest level (e.g. Level 1) starts on the left and the lowest level finishes on the right.

The first letter of any word should be capitalized.

Where applicable, it is appropriate to use titles and numbers together or variants using both. Whatever the case, the arrangement must adhere to convention noted in No. 2.

These guidelines are applicable to both paper and electronic record applications of C-RIMS.



5.6 C-RIMS Corporate Functions and Primaries

Classifications numbers for each level are noted after each level. Levels in bold are corporate Functions (level 1) and levels not in bold are Primaries (level 2)

Executive Functions – 01

- Department Briefing Notes – 01
- Executive Council Briefing Notes – 02
- Briefing Books – 03
- Transition Briefing Books – 04
- Cabinet Papers – 05

Real Property Management – 07

- Design and Construction – 01
- Inventory – 02
- Use and Management – 03
- Disposal - 04

Communication Management -02

- Media Relations – 01
- Advertising – 02
- Internal Communication – 03
- Communication Plan - 04

Information Management and Protection – 08

- Classification and Retention – 01
- Records Inventory – 02
- Information Protection – 03
- Information Protection Breaches – 04
- Record Disposal - 05

Standard – Corporate Records Information Management Standard (C-RIMS)

Financial Management – 03

Accounts Payable – 01
Accounts Receivable – 02
Banking – 03
Budget Planning and Monitoring – 04
Employee Pay and Compensation – 05
Procurement – 06
General Ledger – 07
Financial Delegation - 08

Human Resources Management – 04

Employee Relations – 01
Integrated Disability Management – 02
Organizational Development – 03
Personal File Management – 04
Position Establishment, Classification and Compensation – 05
Staffing and Recruitment – 06
Strategic Human Resource Planning - 07

Asset Management – 05

Asset Inventory – 01
Asset Maintenance – 02
Asset Disposal – 03

Fleet Management – 06

Vehicular Accidents – 01
Fleet Maintenance – 02
Fleet Disposal - 03

Information Technology - 09

IT Service Support – 01
System Development and Maintenance - 02

Safety and Security Management – 10

Emergency Planning – 01
Disaster Recovery – 02
Physical Security – 03
Personnel Security - 04

Compliance Management – 11

ATIPP Request Management – 01
Red Tape Reduction - 02

6.0 C-RIMS Retention and Diposal Schedule

6.1 EXECUTIVE FUNCTIONS – 01

Use for records of the Executive functions of departments. Specifically, for the records of the Offices of Deputy Ministers and equivalents; Assistant Deputy Ministers and equivalents; Chief Executive Officers and Executive Directors.

6.1.1 Department Briefing Notes - 01

Use for records related to briefing notes prepared for and received by Executive and also for briefing notes prepared by an Executive.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Departments

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

EXECUTIVE FUNCTIONS – Department Briefing Notes (01-01)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Department Briefing Notes A briefing note is a short paper that informs a decision-maker about an issue for which he/she are responsible. A good briefing note distills often complex topics into a short well-structured document.</p>	SO	D

6.1.2 Executive Council Briefing Notes – 02

Use for records related to briefing notes prepared for and received by Cabinet Secretariat for the Clerk of the Executive Council.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Executive Council – Cabinet Secretariat

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY+5 and Destroy

Common Secondaries: Refer to [section 5.1](#)

EXECUTIVE FUNCTIONS – Executive Council Briefing Notes (01-02)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Executive Council Briefing Notes A briefing note is a short paper that informs a decision-maker about an issue for which he/she are responsible. A good briefing note distils often complex topics into short, well-structured document.</p>	FY+5	D

6.1.3 Briefing Books – 03

Use for records related to briefing books prepared for and received by Executive and Minister. Such briefing books are created to inform for a particular event, issue and/ or visit (e.g. trip to Labrador for an announcement).

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Departments

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

EXECUTIVE FUNCTIONS - Briefing Books (01-03)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Briefing Book Use for records relating to briefing books prepared for the Executive and/or a Minister.</p>	SO	D

6.1.4 Transition Briefing Books – 04

Use for records related to creation, use, storage and disposal of transition briefing books prepared for a Minister assuming responsibility for a new department.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Departments

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

EXECUTIVE FUNCTIONS – Transition Briefing Books (01-04)			
No.	Function Specific Secondaries	ACT	DIS
41	Transition Briefing Book Use for records relating to briefing books prepared for the Executive and /or a Minister.	SO	D

6.1.5 Cabinet Papers – 05

Use for records related to the Cabinet Submission process. Cabinet Secretariat has the overall responsibility for managing the Cabinet Paper process. Due to high sensitivity of these records, Cabinet Secretariat has very specific requirements in the handling and management of Cabinet Papers by a Non-OPR. Be advised, C-RIMS only documents the retention period of such records. Any other inquiries should be directed to Cabinet Secretariat official(s) in charge of Information Management.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Executive Council – Cabinet Secretariat

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY+10 and to be determined

Common Secondaries: Refer to Refer to [section 5.1](#)

EXECUTIVE FUNCTIONS – Cabinet Papers (01-05)			
No.	Function Specific Secondaries	ACT	DIS
41	Cabinet Paper Use for records relating to the creation of Cabinet Papers. Records include: <ul style="list-style-type: none"> • Correspondence • Presentations • Annexes • Background Material 	FY+10	TBD

6.2 COMMUNICATION MANAGEMENT – 02

Use for records relating to the communications function within government. This does not include the management of communication technologies.

6.2.1 Media Relations - 01

Use for records related to news releases and related material and approval of speeches.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Executive Council – Communications Branch

Departmental OPR: Refer to GNL OPR.

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

COMMUNICATIONS – Media Relations (02-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Mailing and Distribution List Use for records relating to compiling and maintaining media mailing/distribution lists.	SO	D
42	News Release Use for records relating to copies of information released to the media.	SO	D
43	Newspaper Clippings Use for records relating to clipping files of media coverage.	SO	D
44	Media Monitoring Files Use for records relating to interview transcripts, radio transcripts, copies of blogs, clippings from trade journals.	SO	D
45	Polls Use for records relating to creating questions for polling and associated analysis.	SO	D
46	Speeches Use for records associated in the creation and distribution of a Speech by an elected official.	SO	D

6.2.2 Advertising - 02

Use for records related to advertising. This includes promotional materials, public awareness materials, advertising, and approvals.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Executive Council – Communications Branch

Departmental OPR: Refer to GNL OPR

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

COMMUNICATIONS – Advertising (02-02)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Advertising Case Files Use for records relating to advertising on television, radio, internet, newspapers, periodicals, etc. Records include:</p> <ul style="list-style-type: none"> • Promotional Material • Public Awareness Materials • Advertising Material • Approvals 	SO	D

6.2.3 Internal Communication - 03

Use for records related to internal communications in a department.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Departments

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

COMMUNICATIONS – Internal Communications (02-03)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Internal Communications Products Internal newsletters, bulletins, circulars. – Use for widely distributed internal communications.</p>	SO	D

6.2.4 Communication Plan – 04

Use for records related to developing and managing a communications plan.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Departments

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: CY and Destroy

Common Secondaries: Refer to [section 5.1](#)

COMMUNICATIONS – Communication Plan (02-04)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Communication Plan Use for records relating to the development and management of communication plans. Records include:</p> <ul style="list-style-type: none"> • Consultations • Correspondence • Background Material 	CY	D

6.3 FINANCIAL MANAGEMENT – 03

Use for records related to managing the organization’s financial resources. Includes establishing, operating, and maintaining accounting systems and controls and procedures; financial planning; framing budgets and budget submissions; obtaining grants; managing funds in the form of allocations from the Treasury Board; and revenue from charging, trading and investments.

6.3.1 Accounts Payable - 01

Use for records relating to monies owed as the result of a purchase of goods and services. This includes allowances and advances paid (including travel advances), and petty cash, as well as commitments and transaction batches. It also includes accounts payable support documentation (e.g. original invoices, journey authorizations, receiving reports, contracts, etc.); educational allowances, Labrador living allowance, or reimbursement of relocation expenses in accordance with Treasury Board Policy.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Finance

Departmental OPR: Refer to GNL OPR

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Accounts Payable (03-01)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Accountable Advances Use for records relating to purchase in cash less than \$100 value Records include:</p> <ul style="list-style-type: none"> • Interest Accounts • Petty Cash • Travel Authorizations • Travel Advances 	FY	D
42	<p>Accounts Payable Records Use for records relating to supporting documentation that will warrant a payment. Records include:</p> <ul style="list-style-type: none"> • Original Invoice • Contracts • Journey Authorizations 	FY	D
43	<p>Vouchers Use for records relating to the request for payment from Department of Finance for goods or services approved by a department.</p>	FY	D

6.3.2 Accounts Receivable - 02

Use for records relating to the management of funds generated or raised by departments. This includes all revenues from the sale of goods, licenses, permits, fees, etc.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Finance

Departmental OPR: Refer to GNL OPR

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Accounts Receivable (03-02)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Revenue Use for records relating to funds received by a department for services it provides. Records include:</p> <ul style="list-style-type: none"> • Revenue Transactions Reports 	FY	D
42	<p>Taxes Use for records relating to funds received by a department through taxation.</p>	FY	D

FINANCIAL MANAGEMENT – Accounts Receivable (03-02)			
No.	Function Specific Secondaries	ACT	DIS
43	Write-Offs Use for records relating to elimination of outstanding accounts and uncollectible debts, under \$1000 and no court action.	FY	D

6.3.3 Banking - 03

Use for records relating to all regular dealings and transactions with commercial bank institutions.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Finance

Departmental OPR: Refer to GNL OPR

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Banking (03-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Cheques Use for records relating to the payment of funds through the use of cheques.	FY	D

6.3.4 Budget Planning and Monitoring - 04

Use for records relating to the development, preparation and departmental submissions to the Department of Finance of expected or anticipated expenses and revenue within a fiscal year. The budget process is a key area of decision-making in which requests of Department and entities are considered.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Finance

Departmental OPR: Refer to GNL OPR

Schedule: FY+2 and Destroy

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Budget Planning and Monitoring (03-04)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Budget Planning Use for records related to the budget planning process. Records include:</p> <ul style="list-style-type: none"> • Working Papers • Budget Summaries • Internal Analysis Sheets • Expense Summaries • Variance Reports • Compensation Pay Proposals • Budget Request • Budget Submissions 	FY+2	D
42	<p>Budget Change Documentation Use for records relating to the change management process. Records include:</p> <ul style="list-style-type: none"> • Budget Change Forms • Oracle Financial Analysis Updates • Working Papers • Budget Adjustments • Case Proposals 	FY+2	D
43	<p>Budget Monitoring and Forecasting Use for records relating to the monitoring of the disbursements of funds within a fiscal year. Accountabilities include a reporting requirement which is used to ensure funds are disbursed appropriately. Use for records related to the monitoring and forecasting process. Records include:</p> <ul style="list-style-type: none"> • Account Activity Reports • Encumbrances and Expenditure Reports • Detailed List Reports • Budget Status Reports • Working Papers • Forecasting Reports • High Level Oracle Financial Analyzer (OFA) Reviews • Salary Analysis • Legal Costs • Authorizations (i.e. Minute in Council) • Periodic Funding Report 	FY+2	D

FINANCIAL MANAGEMENT – Budget Planning and Monitoring (03-04)			
No.	Function Specific Secondaries	ACT	DIS
44	<p>Special Authorization Requests Use for records relating to the submission and any authorizations of funding within a fiscal year. Records include:</p> <ul style="list-style-type: none"> • Entertainment Exemption Requests • Transfer of Funds Approvals • Special Travel Request • Special Warrant • Authorizations • Treasury Board Minute (TBM) • Minute of Council (MC) 	FY+2	D

6.3.5 Employee Pay and Compensation – 05

Use for records related to information generated or received by departments, agencies or other entities relating to initiation or processing of employee pay and other related employee compensation.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat – Payroll Compensation and Benefits

Departmental OPR: Finance – Office of the Comptroller General (OCG)

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Employee Pay and Compensation(03-05)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Deductions Authorizations Documentation used to start, modify or stop all voluntary or required deductions from payroll, including orders garnishments or other court-ordered attachment.</p>	Original to OCG	D
42	<p>Direct Deposit Applications / Authorizations Authorizations directing deposit information.</p>	Original to OCG	D
43	<p>Earning and Deductions Records Documentation detailing earnings and deductions for each pay period.</p> <ul style="list-style-type: none"> • Individual employee earnings record that show earning and deductions for each pay period. • Master Payroll Register 	SO	D
44	<p>Leave Records Bi-weekly attendance Sheets – Originals to OCG</p>	FY	D

45	Time Sheets Work Schedules and documentation evidencing adherence to or deviation from normal hours for those employees working on fixed schedules – Originals to OCG	FY	D
----	---	----	---

6.3.6 Procurement - 06

Use for records related to acquiring goods and services for GNL. The Government Purchasing Agency (GPA) is the Office of Primary Responsibility (OPR) as it is the central procurement unit for the GNL. GPA functions under the legislative provisions of the *Government Purchasing Agency Act* and the *Public Tender Act*.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Purchasing Agency (GPA)

Departmental OPR: Finance

Schedule: Refer to table below.

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Procurement (03-06)			
No.	Function Specific Secondaries	ACT	DIS
41	Requisitions (Valued at \$2500 or less) Use for records relating to document the details of a purchase requirement by government staff valued at \$2499 or less.	FY+2	D
42	Requisitions (Valued at \$2500 and above) Used for records relating to document the details of a purchase requirement by government staff valued at \$2500 and above. Such requisitions are handled by GPA. Once departments submit their requisition to GPA, these records are deemed copies of convenience.	FY+2	D
43	Tenders (Valued at \$2500 and above) Used for records relating to information used to post a tender, or request for quote, to acquire from buyers a response that is based on purchasing requirements created by government staff. Since GPA manages the posting of all tenders over \$2500, such records held by departments are deemed copies of convenience.	Retain until end of contract then FY+2	D
44	Quotes (Valued at \$2499 or less) Used for records relating to information supplied by a buyer to respond to a request for a quote process. The goods and services quotes are valued at \$2499 or less.	FY+1	D
45	Quotes (Valued at \$2500 and above) Use for records relating to information supplied by a buyer to respond to a request for a quote process. The goods and services quoted are valued at \$2500 and above.	FY+1	D

Standard – Corporate Records Information Management Standard (C-RIMS)

FINANCIAL MANAGEMENT – Procurement (03-06)			
No.	Function Specific Secondaries	ACT	DIS
46	<p>Request for Proposals (RFP) Use for records relating to information used to creating, managing and issuing a RFP. RFP's is a competitive process to ensure the GNL obtains a reasonable price for goods and/or services.</p>	Retain until end of contract then FY+2	D
47	<p>Request for Proposals (RFP) Evaluation Use for records relating to information with conducting an evaluation from a response to an RFP. This includes, but is not limited to:</p> <ul style="list-style-type: none"> • Working Paper Related to Evaluations of Responses • Committee Meeting Minutes • Scorecards • Final Evaluation Report • Committee Notes and Working Papers 	Retain until end of contract then FY+2	D
48	<p>Request for Information (RFI) Use for records relating to information used to with conducting a RFI. RFIs are used to garner whether or not there is interest in the marketplace or to simply gather more information to address a particular sourcing issue for the GNL.</p>	FY+1	D
49	<p>Master Standing Offers (MSO) Use for records relating to creation and management of MSO. MSOs are contracts with a specific supplier for the provision of specific products or services. The scope of a MSO is all government departments. MSO records includes two sub-types: blanket standing offers where each product is listed line by line; and contract standing offers where the details are in an attached document and do not lend themselves to a standard line by line format (e.g., car rental pricing information is included in an attachment).</p>	Retain until end of contract then FY+2	D
50	<p>Master Standing Offers (MSO) Evaluation Use for records relating to information with conducting an evaluation from a response to an MSO. This includes, but is not limited to:</p> <ul style="list-style-type: none"> • Working Paper Related to Evaluations of Responses • Committee Meeting Minutes • Scorecards • Final Evaluation Report • Committee Notes and Working Papers 	Once awarded retain for FY+1	D

Standard – Corporate Records Information Management Standard (C-RIMS)

FINANCIAL MANAGEMENT – Procurement (03-06)			
No.	Function Specific Secondaries	ACT	DIS
51	<p>Individual Standing Offers (ISO) Use for records relating to creation and management of ISO. ISOs are contracts with a specific supplier for the provision of specific products or services. The scope of an ISO is for a specific government department. ISO records includes two sub-types: blanket standing offers where each product is listed line by line; and contract standing offers where the details are in an attached document and do not lend themselves to a standard line by line format (e.g., car rental pricing information is included in an attachment).</p>	Retain until end of contract then FY+2	D
52	<p>Individual Standing Offers (ISO) Evaluation Use for records relating to information with conducting an evaluation from a response to an ISO. This includes, but is not limited to:</p> <ul style="list-style-type: none"> • Working Paper Related to Evaluations of Responses • Committee Meeting Minutes • Scorecards • Final Evaluation Report • Committee Notes and Working Papers 	Once awarded retain for FY+1	D
53	<p>Purchase Orders Use for records related to the creation and management of purchase orders. A purchase order is a procurement tool used by GNL to purchase goods from a supplier. Records include:</p> <ul style="list-style-type: none"> • Standard • Blanket Standing Offer Release • Contract Standing Offer • Encumbered Contract Agreement • Work Order • Aircraft Flight Authorizations • Direct Purchase Order • Travel Order 	FY+2	D
54	<p>Vendor Information Use for records relating to corporations, and businesses. Records include:</p> <ul style="list-style-type: none"> • Contact Information • Product Brochures • Catalogues • Unsolicited Offers of Goods and Services 	SO	D

6.3.7 General Ledger - 07

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Finance

Departmental OPR: Refer to GNL OPR

Schedule: FY+7 and Destroy

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – General Ledger (03-07)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Journal Entry Records Use for records relating to the use and interaction with journal entries which would include correcting previous postings, Interdepartmental journal entries, and public account journal entries.</p>	FY+7	D

6.3.8 Financial Delegation - 08

Use for records related to all matters involving the delegation of authority with financial management

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Finance

Departmental OPR: Refer to GNL OPR

Schedule: Destroy

Common Secondaries: Refer to [section 5.1](#)

FINANCIAL MANAGEMENT – Financial Delegation (03-08)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Temporary Authority Use for records relating to managing financial authorities that are valid for a limited amount of time.</p>	Department s shall not retain a copy	D
42	<p>Signing Authority Delegation Card Use for records relating to managing a specimen signature of a government employee that has been delegated financial authority.</p>	Department s shall not retain a copy	D
43	<p>Cancelled Authorities Use for records relating to cancelling a financial authority.</p>	Department s shall not retain a copy	D

6.4 HUMAN RESOURCES MANAGEMENT – 04

Use for records relating to planning and development of staff. Personnel records are the domain of the Strategic Human Resources Sectors within government, and must be handled outside of this classification plan. Departments should not keep copies of personnel records.

6.4.1 Employee Relations – 01

Use for records related to labour relations and labour standards. Includes collective agreements, strike administration and, grievance procedures (including arbitration and other steps).

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat

Departmental OPR: Refer to GNL OPR

Schedule: Refer to table below.

Common Secondaries: Refer to [section 5.1](#)

HUMAN RESOURCES MANAGEMENT – Employee Relations (04-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Grievances and Arbitration Case Use for records relating to the grievance process at all stages.	1YR after Settlement	SR
42	Labour / Management Committees Use for records relating to Labour/Management Committees.	CY+3	D
43	Collective Agreement Administration Records Use for records relating to the collective process. Records include: <ul style="list-style-type: none"> • Bumping Files • Seniority Listings • Negotiations Planning • Preparation Files • Working Papers 	CY+2	SR
44	Conflict of Interest Case Files Use for records relating to the identification and resolution of employee conflict of interest records. Examples of conflicts may be policy conflicts, contract conflicts, or formal Government guidelines.	CY+2	SR

HUMAN RESOURCES MANAGEMENT – Employee Relations (04-01)			
No.	Function Specific Secondaries	ACT	DIS
45	<p>Employee Supervision and Incident Reporting Use for records relating to the daily managing of employees in the workplace. Records include:</p> <ul style="list-style-type: none"> • Employee Performance Evaluations • Respectful Workplace • Misconduct and Harassment Investigations • Disciplinary Records 	Closure of file Transfer to SHRM	SR to Personal File
46	<p>Employee Family Assistance Programs (EFAP) Records of this type are not permitted to be created under any circumstances. These are to be generated and maintained by the OPR exclusively.</p>	-	-
47	<p>Employee Orientation Information Use for records relating to new employee orientation. Records include orientation schedules, OPR contact information, guidelines, etc. Records include:</p> <ul style="list-style-type: none"> • Orientation Schedules • OPR Contact Information • Guidelines 	SO	D

6.4.2 Integrated Disability Management – 02

Use for records relating to information generated or received by departments, agencies or other entities relating to identification, treatment, rehabilitation and transition back to work of employees from occupational and non-occupational disabilities. These departmental records result from a department’s involvement into a specific issue or general information regarding an Integrated Disability Management area and include all working notes, research information, communications etc.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat

Departmental OPR: Refer to GNL OPR

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

Standard – Corporate Records Information Management Standard (C-RIMS)

HUMAN RESOURCES MANAGEMENT – Integrated Disability Management (04-02)			
No.	Function Specific Secondaries	ACT	DIS
43	<p>Legislative Safety – Related Training Use for records relating specifically to employee safety training programs legislated. Records include:</p> <ul style="list-style-type: none"> • First Aid • WHIMIS • OHS 	CY+1	D
44	<p>OHS Workplace Injury Incident Reports Use for records relating to injury or near injury to government employee.</p>	CY+1	SR
45	<p>OHS Committee Use for records relating to OHS Committees. Records include:</p> <ul style="list-style-type: none"> • Minutes of Meeting • Agenda • Follow-up Notes 	CY+3	D
46	<p>OHS Investigation Case Files Use for records relating to reports to OHS for investigation and hazard conditions. Records include:</p> <ul style="list-style-type: none"> • Original Complaint • Notes • Report • Follow-up Notes 	SO	SR
47	<p>Safety and Prevention Use for records relating specifically to employer safety and prevention measures. Records include:</p> <ul style="list-style-type: none"> • Ergonomics • Promotional Information • Response Planning Measures 	SO	D
48	<p>Workers Compensation Case File Use for records relating to for records relating to an employee WCC incident/claims.</p>	1 year after closure of claim	D
49	<p>Non-Occupational Early Intervention – Sick Leave Tracking Records Use for records relating specifically to the identification of employee absenteeism. Records include:</p> <ul style="list-style-type: none"> • Employee Attendance • Bi-Weekly Reports • Doctors Notes • Case Notes 	n/a	n/a
50	<p>Return to Work Use for records relating specifically to employee return to work option. Records include:</p> <ul style="list-style-type: none"> • Early Intervention Programs 	1 year after follow-up	D

Standard – Corporate Records Information Management Standard (C-RIMS)

HUMAN RESOURCES MANAGEMENT – Integrated Disability Management (04-02)			
No.	Function Specific Secondaries	ACT	DIS
51	Long-term / Short-term Disability Case Files Use for records relating specifically to employee’s inability to return to work and resulting employer accommodations to employee arrangement.	1 year after follow-up	Personal File

6.4.3 Organizational Development – 03

Use for records relating to information generated or received by the departments relating to their organization’s employee development activities, specifically, employee funding, approvals, and departmental strategic learning plans. These departmental records include all working notes, research information, communications, approvals, and funding documents.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat

Departmental OPR: Refer to GNL OPR

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

HUMAN RESOURCES MANAGEMENT – Organizational Development (04-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Legislative Safety Training See Integrated Disability Management	-	-
42	Professional Development and Educational Tools Inventory Corporate information specific to available development programs , web seminars, conferences, video packages, training opportunities, Course evaluations, costs, etc.	SO	D
43	Employee Learning Case Files Use for records relating specifically to the organization’s response to employee development needs. Records include: <ul style="list-style-type: none"> • Requests • Approvals • Notifications • Funding 	SO	D
44	Professional Development Managerial Files Reference information regarding organizational schedules, training locations, etc.	SO	D

HUMAN RESOURCES MANAGEMENT – Organizational Development (04-03)			
No.	Function Specific Secondaries	ACT	DIS
45	<p>Organizational Development Initiative (ODI) Funding Requests / Expenditures Use for records relating specifically to funding of professional development strategies. Records include:</p> <ul style="list-style-type: none"> • Training Costs • Educational Reimbursements • Travel Costs • Accommodations • Vendor Tenders 	SO+3	D

6.4.4 Personal File Management – 04

Use for records related to employee attendance tracking records, performance reviews, peer reviews, letters of disciplinary action, and authorizations of change in salary or rate, copies of employment verifications, copies of requests for changes of address or name, and other pertinent correspondence to or from the employee.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat (HRS)

Departmental OPR: Refer to GNL OPR

Schedule: Refer to table.

Common Secondaries: Refer to [section 5.1](#)

HUMAN RESOURCES MANAGEMENT – Personal File Management (04-04)			
No.	Function Specific Secondaries	ACT	DIS
41	Personal File	-	-

6.4.5 Position Establishment, Classification and Compensation – 05

Use for record related to information generated or received by departments, agencies or other entities relating to identification, requesting or consultation regarding the duties, classification or compensation of a position or employee within their entity. These departmental records include all working notes, research information, communications, etc.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat

Departmental OPR: Refer to OPR

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

HUMAN RESOURCES MANAGEMENT – Position Establishment, Classification and Compensation (04-05)			
No.	Function Specific Secondaries	ACT	DIS
41	Classification Case Files Use for records relating to the evaluation of scope of duties and compensation of new positions.	SO+3	SR
43	Position Case Files Use for records relating specifically to the information gathered in analyzing the need and appropriate salary of a new position.	SO+1	Transfer to CO&M Division
44	Reclassification Case Files Use for records relating to the evaluation of an employee’s duties to determine salary and position designation.	CY+3	D
45	Organizational Chart Listings Updated listings of organizational charts outlining hierarchical relationships in Departments.	SO+1	SR

6.4.6 Staffing and Recruitment – 06

Use for records related to information generated or received by the departments, agencies, boards, etc. or selection members relating to their involvement in staffing activities, specifically, the appointment, promotion, recruitment, screening and selection of candidates within the Public Service. These departmental records include all working notes, research information, communications, evaluations and recommendations etc.

Note: To be determined in phase two (2) review of C-RIMS. Staffing and Recruitment records result from Commission’s obligation under S. 15 (1) (a) of the Public Service Commission Act.

GNL OPR: Public Service Commission (PSC)

Departmental OPR: Refer to GNL OPR

Schedule: Refer to table below.

Common Secondaries: Refer to [section 5.1](#)

HUMAN RESOURCES MANAGEMENT – Staffing and Recruitment (04-06)			
No.	Function Specific Secondaries	ACT	DIS
41	Unsolicited Resumes Use for records relating to resumes sent or delivered to departments not related to specific job competitions.	6 months for date received	D

Standard – Corporate Records Information Management Standard (C-RIMS)

HUMAN RESOURCES MANAGEMENT – Staffing and Recruitment (04-06)			
No.	Function Specific Secondaries	ACT	DIS
42	Competitions Use for records relating to competitions in the filling of positions.	SO	Transfer to PSC upon close of dept. input
43	Applicant Inventories Use for records relating to all student inventories, summer applications, work-term records, articling students, etc.	CY	D
44	Appeal / Investigation Case Files Use for records relating to the appeal and any subsequent investigation into competition process based on individual cases.	SO	Transfer to PSC following end of contribution

6.4.7 Strategic Human Resource Planning - 07

Use for records related to information generated or received by departments, agencies, boards, etc. relating to their organizations' involvement in Human Resource Planning activities. These departmental records include all working notes, research information, communications, approvals, and funding documents.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat

Departmental OPR: Refer to GNL OPR

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

HUMAN RESOURCES MANAGEMENT – Strategic Human Resource Planning (04-07)			
No.	Function Specific Secondaries	ACT	DIS
41	Resource Planning Use for records relating to current human resource inventories and the analysis of supply versus demand forecasting.	SO	SR
42	Work Plan File – Departmental Use for records relating to the strategic planning activities of a Department respecting its current and future professional needs.	SO+5	SR
43	Work Plan File – Corporate Records relating to the overall corporate objectives and the complimenting HR activities to achieve these objectives.	SO	SR

HUMAN RESOURCES MANAGEMENT – Strategic Human Resource Planning (04-07)			
No.	Function Specific Secondaries	ACT	DIS
44	Consultative Services Records relating to the daily activities of receiving direction respecting HR planning activities.	SO	D

6.5 ASSET MANAGEMENT – 05

Use for records related to the management, maintenance, and disposal of assets, excluding fleet and real property assets. This includes maintenance agreements, improvements, warranties, depreciation tracking, lease management, etc.

Under section 15 of the *Executive Council Act*, a department has the responsibility to inventory, track, maintain and dispose of Fixed Assets.

6.5.1 Asset Inventory - 01

Use for records relating to information about the accountability for receipt, storage, stock inventory, and issue of equipment. Includes stock-taking control, procedures, and transaction records, for example: transfer vouchers and inventory reports.

Fixed assets include all non-consumable moveable items with a useful life of one year or more. Equipment items are used in normal daily operations and are not for resale purposes. Computer equipment is not included in Fixed Asset inventories.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Refer to GNL OPR

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

ASSET MANAGEMENT – Fixed Asset Inventory (05-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Annual Inventory Records Records include control sheets, control record logs, tag records etc.	SO	D
42	Inventory Adjustment Forms Copies of completed forms outlining any changes in location, etc. to particular fixed assets	SO	D
43	Inventory Temporary Relocations Use for records relating to any changes in inventory relocations, include equipment on loan to other locations, or transferred to another location.	SO	D

ASSET MANAGEMENT – Fixed Asset Inventory (05-01)			
No.	Function Specific Secondaries	ACT	DIS
44	<p>Fixed Inventory Audits</p> <p>Use for records relating to the auditing process of inventory records by the OPR. Records include:</p> <ul style="list-style-type: none"> • Audit Notifications • Documentation Requests • Responses 	SO	D

6.5.2 Asset Maintenance – 02

Use for records relating to information about daily upkeep and repair of equipment and furnishings. Includes: standing offer agreements, work orders, price lists, and suppliers’ catalogues. Examples include technical specifications, equipment catalogues, and vendor literature.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

ASSET MANAGEMENT – Asset Maintenance (05-02)			
No.	Function Specific Secondaries	ACT	DIS
41	<p>Vendor Information</p> <p>Use for records relating to vendors. Records include:</p> <ul style="list-style-type: none"> • Vendor Contact Information • Promotional Material • Company Profile 	SO	Review and Purge Annually
42	<p>Replacement / Evaluation Files</p> <p>Use for records relating to the evaluation, repair and/or replacement of fixed assets.</p>	SO	D

6.5.3 Asset Disposal - 03

Use for records relating to the removal and disposal of assets. This includes assets deemed to be surplus and are scheduled for transfer and/or disposal actions such as an auction.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Purchasing Agency

Departmental OPR: Transportation and Works

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

ASSET MANAGEMENT – Asset Disposal (05-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Transfers to Surplus Listings of equipment no longer needed by a department which is transferred to Surplus inventory for disposal or reuse.	SO	D
42	Obsolete / Damaged Items Listings Includes all disposition forms, etc. related to the process of evaluation of fixed assets.	SO	D
43	Fixes Asset Reconciliation Reconciliation of previous year-end general fixed assets listing to current year-end general fixed assets listing	SO	D
44	Disposition Authorization Requests Requests for authorization to dispose of equipment.	SO	D
45	Lost and Stolen Reports Use for records relating to the reporting of asset(s) being lost or stolen.	SO	D

6.6 FLEET MANAGEMENT – 06

Use for records related to maintaining, repairing and disposing of vehicles. Vehicles include any means of conveyance owned or used by the organization to transport people or items.

6.6.1 Vehicular Accidents – 01

Use for records relating to injury or damage caused by vehicles. Includes damages or injury incurred by staff en route to, from, or at work, and includes accident prevention.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Transportation and Works

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

FLEET MANAGEMENT – Vehicular Accidents (06-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Vehicular Accident Case Files Use for records relating to a vehicle accident involving a government employee and/or non-employees. Records include: <ul style="list-style-type: none"> • Repairs Needed • Repairs 	1 Year after settlement of claim	D

6.6.2 Fleet Maintenance – 02

Use for records relating to the activities associated with the upkeep, repair and preservation of a vehicle.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Transportation and Works

Schedule: Destroy

Common Secondaries: Refer to [section 5.1](#)

FLEET MANAGEMENT – Fleet Maintenance (06-02)			
No.	Function Specific Secondaries	ACT	DIS
41	Vehicular Maintenance Case Files Use for records relating to the maintenance of the vehicle. Records include: <ul style="list-style-type: none"> • Log of oil changes 	Do not retain	D

6.6.3 Fleet Disposal - 03

Use for records relating to the process of disposing of vehicles no longer required by the organization, by sale, transfer, termination of lease, auction, or destruction.

Note: To be determined in phase two (2) review of C-RIMS.

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

FLEET MANAGEMENT – Fleet Disposal (06-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Fleet Disposal Case Files Use for records relating to preparing and managing the disposal of vehicles. This includes records used to create a tender for disposal.	FY	D

6.7 REAL PROPERTY MANAGEMENT – 07

Use for records relating to the management of real property such as buildings, lands and infrastructure (including inventories, property records and leases).

6.7.1 Design and Construction – 01

Use for records relating to major modification or expansion of existing structures through construction.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Transportation and Works

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

REAL PROPERTY MANAGEMENT – Design and Construction (07-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Building Plans Use for records relating to the plans and diagrams for the construction and renovation of buildings. Also includes revisions made after construction has started.	SO	D
42	Construction Case Files Use for records relating to individual construction project case files. This includes major renovations.	CY	D
43	Specifications Use for records relating to the materials and methods specifications for the construction and renovation of buildings. Also include revisions made after construction has started.	CY	D

6.7.2 Inventory – 02

Use for records relating to space and real property holdings of a department. Includes inventories of land owned or used by a department, property, occupied space and use inventories, and supporting documents.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Transportation and Works

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

REAL PROPERTY MANAGEMENT – Inventory (07-02)			
No.	Function Specific Secondaries	ACT	DIS
41	Facilities Inventory Case Files Use for records relating to facilities utilized by each department. Includes details related to lease expiry dates. Includes files related to renovations required for organizational moves.	SO	D
42	Land Inventory Case Files Use for records relating to maintenance of grounds and repair projects.	SO	D
43	Property Inventory Case Files Use for records relating to property utilized by each department.	SO	D

6.7.3 Use and Management – 03

Use for records relating to the upkeep, repair, and servicing of government-owned facilities. Includes janitorial and cleaning services; elevator maintenance contracts and elevator inspection reports; operation, maintenance, repairs and inspection reports of utility systems and facilities. Utility systems include air conditioning, ventilation, heating and other environmental control systems; oil, propane, gas systems; lighting and electrical systems; and water and plumbing systems.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Transportation and Works

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

REAL PROPERTY MANAGEMENT – Use and Management (07-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Janitorial / Cleaning Services Use for records relating to cleaning and basic up-keep of government buildings.	FY	D
42	Basic Maintenance Use for records relating to basic maintenance and repairs to government buildings.	FY	D
43	Utilities Use for records relating to the operation and maintenance of utility systems such as air conditioning, garbage disposal, lighting, plumbing and heating, etc.	FY	D
44	Recycling Use for records relating to all recycling activities associated with property management. Includes cardboard, paper, etc.	FY	D
45	Land Maintenance Case Files Use for records relating to specific land maintenance projects.	FY	D
46	Floor Layouts Records related to managing floor layouts.	SO+2	D

6.7.4 Disposal - 04

Use for records related to the disposal of real property through any means. Examples include Tender of Real Property; working files related to disposal of Real Property.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Government Purchasing Agency

Departmental OPR: Transportation and Works

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

REAL PROPERTY MANAGEMENT – Disposal (07-04)			
No.	Function Specific Secondaries	ACT	DIS
41	Disposal Case Files Use for records related to the disposal of government buildings. This includes tendering for disposal records.	FY	D

6.8 INFORMATION MANAGEMENT AND PROTECTION – 08

Use for records relating to the administration and management functions associated with records and information within departments. This primary may also be known as “records

Standard – Corporate Records Information Management Standard (C-RIMS)

management” or as” records and information management”. It also includes functions related to the protection of information in all forms.

6.8.1 Classification and Retention – 01

Use for records relating to corporate records classification and retention plans.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Office of the Chief Information Officer (OCIO) – Corporate and Information Management Services Branch (CIMS)

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: <Insert Disposition if common across all function specific secondaries. Otherwise refer to table below.>

Common Secondaries: Refer to [section 5.1](#)

INFORMATION MANAGEMENT AND PROTECTION – Classification and Retention (08-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Classification System Development Use of records related to the development of a file classification system for records.	FY	D
42	Classification Plan Use for records related to the management of a file classification plan.	-	TBD

6.8.2 Records Inventory – 02

Use for inventories (including electronic inventories) of active, semi-active or inactive records. Inventories of records in commercial storage.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Office of the Chief Information Officer (OCIO) – Corporate and Information Management Services (CIMS) Branch

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

Standard – Corporate Records Information Management Standard (C-RIMS)

INFORMATION MANAGEMENT AND PROTECTION – Records Inventory(08-02)			
No.	Function Specific Secondaries	ACT	DIS
41	Records Inventory Lists (Active) Use for records relating to file listing or inventories of records in current regular use.	FY	D
42	Records Inventory Lists (Semi-Active) Use for records relating to listings of a department’s semi-active records holdings.	FY	D

6.8.3 Information Protection – 03

Use for records related to managing information security and protection efforts. This includes Privacy Impact Assessment.

Note: To be determined in phase two (2) review of C-RIMS

GNL OPR: Office of the Chief Information Officer (OCIO) – Corporate and Information Management Services (CIMS) Branch

Departmental OPR: Office of the Chief Information Officer (OCIO) – Corporate and Information Management Services (CIMS) Branch

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

INFORMATION MANAGEMENT AND PROTECTION – Information Protection (08-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Oaths of Secrecy Use for records relating to administering and managing information used with Oaths of Secrecy taken by employees and contractors.	FY	D
42	Privacy Impact Assessment Use for records relating to administering and managing a Privacy Impact Assessment. This includes Preliminary Privacy Impact Assessments.	FY	D

6.8.4 Information Protection Breaches – 04

Use for records relating to security and privacy breaches. Includes breach reports and investigations records.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Office of the Information and Privacy Commissioner (OIPC)

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

INFORMATION MANAGEMENT AND PROTECTION – Information Protection Breaches (08-04)			
No.	Function Specific Secondaries	ACT	DIS
41	Information Protection Breach Case Files Used for records relating to methods and procedures required in handling an information protection breach.	FY	D

6.8.5 Record Disposal - 05

Use for records related to corporate information disposed of by a department. This includes Certificates of Destruction.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Office of the Chief Information Officer (OCIO) – Corporate and Information Management Services (CIMS) Branch

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

INFORMATION MANAGEMENT AND PROTECTION – Records Disposal (08-05)			
No.	Function Specific Secondaries	ACT	DIS
41	Destroyed Records Inventory Use for records relating to lists of records which, following authorization have been destroyed.	FY	D
42	Disposal Authorization Use for records relating to the approval notification from the Public Records Committee for removal of records from the Department. This includes authorization to destroy records or transfer to the Rooms.	FY	D
43	Records Retention and Disposal Schedules (RRDS) Use for records relating to departmental copies of retention and disposal schedules approved for records.	FY	D

6.9 INFORMATION TECHNOLOGY – 09

Use for records relating to the planning, use and ongoing management of Information Technology (IT) assets, systems, policies, procedure and standards.

6.9.1 IT Service Support – 01

Use for records relating to the request for support to address problems with computer applications (e.g., password reset), networks, IT assets, or any other type of request that is handled by the IT Help Desk.

Note: To be determined in phase two (2) review of C-RIMS. Non-OCIO staff that may have dealing with the OCIO in order to resolve a problem with computer applications, networks, or IT assets.

GNL OPR: Office of the Chief Information Officer (OCIO)

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

INFORMATION TECHNOLOGY (IT) – IT Service Support (09-01)			
No.	Function Specific Secondaries	ACT	DIS
41	IT Service Request Use for records relating to departmental requests for IT assistance.	FY	D

6.9.2 System Development and Maintenance – 02

Use for records relating to IT system development and maintenance. This includes the computer software applications and networks.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Office of the Chief Information Officer (OCIO)

Departmental OPR: Office of the Chief Information Officer (OCIO)

Schedule: FY+2 and Destroy

Common Secondaries: Refer to [section 5.1](#)

INFORMATION TECHNOLOGY (IT) – System Development and Maintenance (09-02)			
No.	Function Specific Secondaries	ACT	DIS
41	IT Project Case Files Use of records the management of an IT project managed by the OCIO.	FY+2	D

6.10 SAFETY AND SECURITY MANAGEMENT – 10

Use for records relating to the management of personal safety and security for government.

6.10.1 Emergency Planning – 01

Use for emergency plans and procedures internal to departments, planning for response to provincial crises, evacuation plans, business continuity and business resumption plans.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Municipal Affairs – Fire and Emergency Services (FES)

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

SAFETY AND SECURITY MANAGEMENT – Emergency Planning (10-01)			
No.	Function Specific Secondaries	ACT	DIS
41	Evacuation Plans Use for records relating to evacuation plans and procedures resulting from fire or other hazards.	SO	D
42	Fire Prevention Use for records relating to fire prevention measures within Government departments and buildings.	SO	D

6.10.2 Disaster Recovery – 02

Use for records relating to disaster recovery internal to departments, planning for response to provincial crises, evacuation plans, business continuity and business resumption plans.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Municipal Affairs - Fire and Emergency Services

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

SAFETY AND SECURITY MANAGEMENT – Disaster Recovery (10-02)			
No.	Function Specific Secondaries	ACT	DIS
41	Disaster Recovery (DR) Plans Records relating to plans for the continuation of operations in the event of a disaster or emergency and procedures to recover.	FY	D
42	Business Continuity Plans (BCP) Records relating to plans and procedures to maintain operations in the event of a disaster or emergency and procedures to recover.	FY+1	D

6.10.3 Physical Security – 03

Use for records relating to control and safeguards on physical access to departmental buildings, including threat and risk assessment, guard services, contingency planning, investigations of security breaches and violations, protection, theft, and vandalism.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Transportation and Works

Departmental OPR: Transportation and Works

Disposition: Refer to table below

Common Secondaries: Refer to [section 5.1](#)

SAFETY AND SECURITY MANAGEMENT – Physical Security (10-03)			
No.	Function Specific Secondaries	ACT	DIS
41	Facility Access Files (Visitor Log) Use for records relating to the documenting of a visitor (government and non-government employee) to a government building.	FY+1	D
42	Incident Case Files Use for records relating to specific incidents of security breaches.	FY	D

6.10.4 Personnel Security - 04

Use for records relating to administration of security clearances and reliability checks on government employees and contractors, building passes, employee identification cards, and visitors.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Human Resource Secretariat

Departmental OPR: Human Resource Secretariat

Schedule: FY and Destroy

Common Secondaries: Refer to [section 5.1](#)

SAFETY AND SECURITY MANAGEMENT – Personnel Security (10-04)			
No.	Function Specific Secondaries	ACT	DIS
41	Identification Cards Use of records in the collection and management of information related to the identification cards by employees and contractors. Such cards are used to gain access to government facilities	FY	D

6.11 COMPLIANCE MANAGEMENT – 11

Use for records relating to the activities associated with complying with mandatory or optional accountability, fiscal, legal regulatory or quality standards or requirements. Includes compliance with legislation, national and international standards, audit, red tape reduction, etc.

6.11.1 ATIPP Request Management – 01

Use for records relating to Access to Information and Protection of Privacy (ATIPP) requests and all of the files compiled to respond to requests in accordance with the Access to Information and Protection of Privacy Act. Requests must be handled according to the requirements of the Office of the ATIPP Coordinator, Department of Justice.

Note: To be determined in phase two (2) review of C-RIMS.

GNL OPR: Office of Public Engagement (OPE) – Access to Information and Protection of Privacy (ATIPP) Office

Departmental OPR: Departmental Executive, including Deputy Minister, Assistant Deputy Minister, and Executive Directors, who have responsibility for a particular departmental branch, function, and or program/service.

Schedule: FY+1 and Destroy

Common Secondaries: Refer to [section 5.1](#)

COMPLIANCE MANAGEMENT – ATIPP Request Management (11-01)			
No.	Function Specific Secondaries	ACT	DIS
41	ATIPP Request Case Files Use for records relating to methods and procedures required in handling an ATIPP request.	FY+1	D

6.11.2 Red Tape Reduction - 02

Use for records related to managing Red Tape Reduction commitments set out for departments.

Note: To be determined in phase two (2) review of C-RIMS

GNL OPR: Service NL

Departmental OPR: To Be Determined (TBD)

Schedule: SO and Destroy

Common Secondaries: Refer to [section 5.1](#)

COMPLIANCE MANAGEMENT – Red Tape Reduction (11-02)			
No.	Function Specific Secondaries	ACT	DIS
41	Red Tape Reduction Reporting Use for records relating to reporting the RTR Office on efforts by the Department to comply with the RTR initiative.	SO	D

7.0 Roles and Responsibilities

Role of the CIMS, OCIO

The CIMS is mandated to provide advisory services to government departments; develop IM policies and standards; lead strategic IM initiatives for the GNL; and build IM capacity within the GNL.

Role of The Rooms Provincial Archives

The Rooms Provincial Archives role in the management of the records of public bodies is threefold. It is responsible for the archival appraisal of the records of public bodies; the preservation of archival records of public bodies and for making those records available for research use.

Role of the IM Directors Forum

The IM Directors Forum is an advisory body to the OCIO. It is comprised of senior IM professionals and provides input for OCIO policy and standards development and acts in a senior advisory capacity on matters of direction and focus. It is also a key group through which the OCIO disseminates policy, standards and communications for the GNL.

8.0 Definitions and Acronyms

8.1 Definitions

<i>Government Records Committee</i>	The Government Records Committee (GRC) is the official body that is mandated to: (1) Review and revise schedules for the retention, disposal, destruction or transfer of government records;(2) Make recommendations to the minister respecting public records to be forwarded to The Rooms, Provincial Archives; (3) Authorize disposal and destruction standards and guidelines for the lawful disposal and destruction of public records; and (4) Make recommendations to the minister regarding the removal, disposal and destruction of records (source: <i>Management of Information Act SNL2005 c.M-1.01</i>).
--	---

<p><i>Office of Primary Responsibility</i></p>	<p>The Office of Primary Responsibility (OPR) is the organization and/or position within an organization that is responsible for maintaining the integrity of a record (source: Corporate Records and Information Management Standard (C-RIMS)).</p>
--	--

8.2 Acronyms

CIMS	Corporate and Information Management Services
C-RIMS	Corporate Records Information Management Standard
GNL	Government of Newfoundland and Labrador
GRC	Government Records Committee
IM	Information Management
IMSAR	Information Management Standard for Administrative Systems
OCIO	Office of the Chief Information Officer
RRDS	Records Retention and Disposal Schedule

9.0 Compliance and Enforcement

Mandatory compliance

OCIO Standards are mandatory for users to follow and dictate uniform ways of operating.

Compliance monitoring

Compliance monitoring of this Standard is the responsibility of the Department.

Penalty for failure to comply

Willful non-compliance with this Standard, including contravention through negligence, may result in disciplinary action, up to and including termination of employment, contract or access.

10.0 Monitoring and Review

The (Issuing Branch) is responsible for monitoring and reviewing this Standard in accordance with processes set forth by the Corporate and Information Management Services Branch.

11.0 References

Management of Information Act

Rooms Act

Information Management and Protection Policy, TBM 2009-335

12.0 Revision History

Version	Date Reviewed	Reviewed By
01	2009-10-06	Porter, Kim – Coordinator, GRLM GRC Meeting 2009-08
02	2016-04-12	Porter, Kim – Coordinator, GRLM GRC Meeting 2016-004

13.0 Appendices

Appendix A:	Template Memorandum for C-RIMS Implementation
Appendix B:	Corporate Records and Information Management (C-RIMS) FAQ's

Appendices are available online on OCIO's [website](#).

Index

Accountable Advances	19	Direct Deposit Applications /	
Accounts Payable - 01	18	Authorizations	22
Accounts Payable Records	19	Disaster Recovery – 02	47
Accounts Receivable - 02	19	Disaster Recovery (DR) Plans	47
Advertising - 02	16	Disposal - 04	41
Advertising Case Files	17	Disposal Authorization	45
Annual Inventory Records	35	Disposal Case Files	41
Appeal / Investigation Case Files	33	Disposition Authorization Requests	36
Applicant Inventories	33	Earning and Deductions Records	22
Asset Disposal - 03	36	Emergency Planning – 01	46
Asset Inventory - 01	34	Employee Family Assistance Programs	
Asset Maintenance – 02	35	(EFAP)	28
ASSET MANAGEMENT - 05	34	Employee Learning Case Files	31
ATIPP Request Case Files	49	Employee Orientation Information	28
ATIPP Request Management – 01	49	Employee Relations – 01	27
Banking - 03	20	Employee Supervision and Incident	
Basic Maintenance	41	Reporting	28
Briefing Book	14	Evacuation Plans	47
Briefing Books – 03	14	Executive Council Briefing Notes	14
Budget Change Documentation	21	Executive Council Briefing Notes – 02	13
Budget Monitoring and Forecasting	21	Facilities Inventory Case Files	40
Budget Planning	21	Facility Access Files (Visitor Log)	48
Budget Planning and Monitoring - 04	20	Financial Delegation - 08	26
Building Plans	39	FINANCIAL MANAGEMENT - 03	18
Business Continuity Plans (BCP)	47	Fixed Inventory Audits	35
Cabinet Paper	15	Fixes Asset Reconciliation	36
Cabinet Papers – 05	15	Fleet Disposal - 03	38
Cancelled Authorities	26	Fleet Disposal Case Files	39
Cheques	20	Fleet Maintenance – 02	38
Classification and Retention – 01	42	FLEET MANAGEMENT – 06	36
Classification Case Files	32	Floor Layouts	41
Classification Plan	42	General Ledger - 07	25
Classification System Development	42	Grievances and Arbitration Case	27
Collective Agreement Administration		Identification Cards	49
Records	27	Incident Case Files	48
COMMUNICATION MANAGEMENT - 02	16	Individual Standing Offers (ISO)	25
Communication Plan	18	Individual Standing Offers (ISO)	
Communication Plan – 04	17	Evaluation	25
Competitions	33	INFORMATION MANAGEMENT AND	
COMPLIANCE MANAGEMENT – 11	49	PROTECTION – 08	42
Conflict of Interest Case Files	27	Information Protection – 03	43
Construction Case Files	39	Information Protection Breach Case Files	
Consultative Services	34	44
Deductions Authorizations	22	Information Protection Breaches – 04	43
Department Briefing Notes	7, 8, 13	INFORMATION TECHNOLOGY – 09	45
Department Briefing Notes - 01	13	Integrated Disability Management – 02	28
Design and Construction – 01	39	Internal Communication - 03	17
Destroyed Records Inventory	45	Internal Communications Projects	17
		Inventory – 02	39

Standard – Corporate Records Information Management Standard (C-RIMS)

Inventory Adjustment Forms	35	Quotes (Valued at \$2499 or less)	23
Inventory Temporary Relocations	35	Quotes (Valued at \$2500 and above)	23
IT Project Case Files	46	REAL PROPERTY MANAGEMENT – 0739	
IT Service Request	46	Reclassification Case Files	32
IT Service Support – 01	45	Record Disposal - 05	44
Janitorial / Cleaning Services	41	Records Inventory – 02	42
Journal Entry Records	26	Records Inventory Lists (Active)	43
Labour / Management Committees	27	Records Retention and Disposal	
Land Inventory Case Files	40	Schedules (RRDS)	45
Land Maintenance Case Files	41	Recycling	41
Leave Records	22	Red Tape Reduction - 02	50
Legislative Safety – Related Training	29	Red Tape Reduction Reporting	50
Legislative Safety Training	31	Replacement / Evaluation Files	36
Long-term / Short-term Disability Case		Request for Information (RFI)	24
Files	30	Request for Proposals (RFP)	24
Lost and Stolen Reports	36	Request for Proposals (RFP) Evaluation	
Mailing and Distribution List	16	24
Master Standing Offers (MSO)	24	Requisitions (Valued at \$2500 and	
Master Standing Offers (MSO) Evaluation		above)	23
.....	24	Requisitions (Valued at \$2500 or less)	23
Media Monitoring Files	16	Resource Planning	34
Media Relations - 01	16	Return to Work	29
News Release	16	Revenue	19
Newspaper Clippings	16	SAFETY AND SECURITY MANAGEMENT	
Oaths of Secrecy	43	– 10	46
Obsolete / Damaged Items Listings	36	Safety Prevention	29
OHS Committee	29	Signing Authority Delegation Card	26
OHS Investigation Case Files	29	Special Authorization Requests	22
OHS Workplace Injury Incident Reports		Specifications	39
.....	29	Speeches	16
Organizational Chart Listings	32	Staffing and Recruitment – 06	32
Organizational Development – 03	30	Strategic Human Resource Planning - 0733	
Organizational Development Initiative		Taxes	19
(ODI) Funding Requests / Expenditures		Temporary Authority	26
.....	31	Tenders (Valued at \$2500 and above)	23
Payroll – 05	22	Time Sheets	23
Personal File	32	Transfers to Surplus	36
Personal File Management – 04	31	Transition Briefing Book	15
Personnel Security - 04	48	Transition Briefing Books – 04	14
Physical Security – 03	47	Unsolicited Resumes	33
Position Case Files	32	Use and Management – 03	40
Position Establishment, Classification and		Utilities	41
Compensation – 05	32	Vehicular Accident Case Files	38
Privacy Impact Assessment	43	Vehicular Accidents – 01	37
Procurement - 06	23	Vehicular Maintenance Case Files	38
Professional Development and		Vendor Information	25, 35
Educational Tools Inventory	31	Vouchers	19
Professional Development Managerial		Work Plan File – Corporate	34
Files	31	Work Plan File – Departmental	34
Property Inventory Case Files	40	Workers Compensation Case File	29
Purchase Orders	25	Write-Offs	19



6. Guidelines

6.1. GNL Email Guidelines	15
6.2. Discovery and Legal Hold	16
6.3. Managing Departmental Information through the Employment Cycle	17
6.4. Managing the Records of External Public Bodies	18


					
Document Title: Government of Newfoundland and Labrador Email Guidelines					
Document Type: Guidelines					No. Of Pages 19
Scope: Government of Newfoundland Labrador					
Trim #		Revision # 10		Treasury Board Approval (#) TBM2009-298	
Supersedes Email Policy previously approved by TBM 2006-157					
2009-02-03	2009-10-08	2011-10-08	Shelley Smith Office of the Chief Information Officer (OCIO)	Jean Tilley	Secretary
Date Created	Approval Date	Expiry Date	Lead Branch - Name Information Management Branch	Policy and Planning	Treasury Board Approval

Table of Contents

1.0	Why do we have email guidelines?	4
1.1	Purpose	4
1.2	Scope.....	4
2.0	What are the individual’s responsibilities?.....	5
3.0	Management of email messages.....	6
3.1	Email government records	6
3.1.1	Which email messages are government records?	6
3.1.2	Who is responsible to keep email government records?	7
3.1.3	Are email copies considered government records?	7
3.1.4	Which email messages are transitory records?	8
3.1.5	Backup and retention of email	8
3.2	How do I file email?	9
3.2.1	What is an Electronic Document Management System (EDMS)?	9
3.2.2	Records offices and hard copy files.....	9
3.3	When can I destroy email messages?.....	9
3.3.1	When can I get rid of email government records?.....	10
3.3.2	When can I destroy email transitory records?	10
3.3.3	Deleting email	10
3.4	Responsibilities of departing/moving employees.....	10
3.4.1	Managers’ Responsibility	11
3.4.2	Removal of email accounts	11
3.4.3	Abandoned Email Disposal Process	12
4.0	Creating and using email.....	13
4.1	How to use email effectively.....	13
4.1.1	Misuse of email.....	13
4.2	Who owns email on the Government of Newfoundland and Labrador system? 13	
4.3	What legislation applies to email?.....	13
4.4	Legal issues	13
4.5	Can anyone gain access to a user’s email?	14
4.5.1	Monitoring of email	14
	Access to email by system administrators	14
4.5.2	Email system audit trails	15

Government of Newfoundland and Labrador Email Guidelines

4.6 Privacy..... 15

4.7 Security 15

4.7.1 Security of Attachments 15

5.0 References 16

5.1 Relevant Legislation..... 16

5.2 Policies 16

6.0 Key Contacts..... 17

Appendix 1 – Glossary and Terms 18

1.0 Why do we have email guidelines?

Electronic mail (email) is a means of sending messages between computers using electronic networks and includes sending and receiving messages through the use of government's internal email systems as well as sending and receiving messages across the Internet. It is an integral part of doing business today, effectively replacing a large number of telephone calls, memos, and letters.

With the daily use of email throughout government and society at large, users transmit more and more information electronically without the use of paper documents. This requires the use of effective information management practices in the creation, use and management of email messages, including the identification and retention of emails which are official government records as defined in the *Management of Information Act* and the *Rooms Act*.

1.1 Purpose

The Government of Newfoundland and Labrador is committed to delivering services through electronic means. The purpose of these guidelines is to identify the requirements for proper and responsible management and use of email by public employees and contractors working on behalf of Government of Newfoundland and Labrador. The guidelines recognize email as a valuable resource as a communications medium, and as a tool for disseminating departmental information and facilitating decision-making.

1.2 Scope

These guidelines are applicable to all Government of Newfoundland and Labrador employees and individuals contracted to work for it. This includes all executive, management, unionized and non-unionized levels, who are authorized users of Government of Newfoundland and Labrador email systems, as well as anyone authorized to work on behalf of Government of Newfoundland and Labrador, such as contractors and student employees.

All the information collected or created in the conduct of business for the government is the property of Government of Newfoundland and Labrador, including emails sent and received in the conduct of business either as an employee or contractor of Government of Newfoundland and Labrador.

Furthermore, all Information Technology (IT) systems, infrastructure and software provided by Government of Newfoundland and Labrador is the property of Government of Newfoundland and Labrador, and can be monitored as required, by authorized Government of Newfoundland and Labrador employees. These guidelines apply whether the user is using government equipment, his/her own equipment, or equipment belonging to a third party.

2.0 What are the individual's responsibilities?

Information collected or created in the conduct of business by users of the Government of Newfoundland and Labrador email system is the property of the Government of Newfoundland and Labrador. All users are responsible for the following:

- creating, using, communicating and sharing email messages according to these guidelines;
- retaining government records, in the format and media required by the department and organized in a way that makes them accessible to those authorized to view the contents;
- removing records of a personal or transitory nature from email systems on a regular and timely basis;
- protecting all email government records from unauthorized disclosure to third parties and from inadvertent loss or destruction;
- protecting the personal information of public employees and government clients or citizens in government email messages according to the requirements of the Access to Information and Protection of Privacy Act and government policy;
- disposing of email government records according to authorized records retention and disposition schedules;
- ensuring that, particularly when dealing with sensitive information, the email is sent only to the correct recipient(s),
- ensuring the email addresses of recipients are correct;
- verifying that a distribution list is up-to-date and that the recipients for a particular message are authorized to receive the message before sending it to an entire list; and
- not forwarding another user's email message to a discussion group, Listserv™, newsgroup or posting it on an electronic bulletin board without the user's permission.

Managers are responsible to ensure that all users (including contractors, students, temporary help, etc.) under their supervision, who have access to the departmental email system, read and comply with these guidelines, and that email government records of departing users (either from the department or their operational area) are retained, filed and accessible to meet legislative, departmental business and accountability requirements.

Information systems managers are responsible for providing a means to transmit and store email messages. They are also responsible for ensuring that these email

Government of Newfoundland and Labrador Email Guidelines

messages are preserved and protected from destruction or unauthorized access and that email is securely destroyed once authorization has been acquired.

Information Management Branch, Office of the Chief Information Officer, is responsible for ensuring that users are informed about these guidelines, for publishing them on the Government of Newfoundland and Labrador Intranet and for providing expert advice and guidance on the identification, filing, retention protection and disposal of email records.

3.0 Management of email messages

Along with information in other formats, email messages must be managed with consideration for legislative and policy requirements, and the requirements to provide evidence of business activity. A user should ensure that his/her computer is not left unsecured and that he/she does not share his/her password(s) with others.

Email messages which are government records, as defined in the *Management of Information Act*, must be organized and managed to be easily retrievable and disposed of only in accordance with the provisions of Section 5 of the *Act*. It is the responsibility of the department in cooperation with the Office of the Chief Information Office to store, manage, retrieve, preserve, protect, dispose and transfer email records of employees who have left the department.

Email messages that are transitory records may be deleted once this information is no longer required.

3.1 Email government records

3.1.1 Which email messages are government records?

Email constitutes government records if they contain messages created, sent or received by a department that are required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities that document Government of Newfoundland and Labrador business. **These must be managed in the same way as government records in other media, such as paper.**

When email messages fit **any** of the following criteria they **are** government records:

- required to maintain business operations (e.g., emails giving instructions about critical operations or policy direction);
- initiate, authorize, document, complete or provide evidence of a business transaction(s) (e.g., documenting a final decision on an issue);
- protect the rights of citizens and/or the government (e.g., relate to an individual citizen's or group of citizen's relationship with the government – as a client for example);
- provide evidence of compliance with accountability or other business requirements (e.g., document adherence to government policy or provide decision-making trails);

Government of Newfoundland and Labrador Email Guidelines

- have potential business, legal, research or archival value (e.g., document the development of decision, policy or creation of briefing materials);
- reflect the position or business of the department or government (e.g., an email to a citizen stating the department's position or policy on a particular issue);
- original messages of policies or directives (i.e., not a message on which the recipient is merely one of many people receiving copies) and, when the information does not exist elsewhere (for example, when the recipient is not merely one of many people copied on the message); and
- messages related to employee work schedules and assignments (e.g., an email requesting that a staff person work over time).

3.1.2 Who is responsible to keep email government records?

The originator (creator) of an email is responsible to ensure that official email government records are retained and managed. This requirement also applies for recipients of email messages sent from external sources, where the information contained in the email does not exist elsewhere in the department, and it forms part of the departmental record. In such cases, that externally generated email will become a government record.

When an originator creates an email message for response from one or several recipients, he/she is also responsible to ensure that the original text and all responses that form the complete email government record are retained.

Emails generated to enable collaboration and information sharing within committees, working groups or work teams do not necessarily need to be retained by all members of the group. The best approach in such situations is to have one member of the group be the "keeper of the records". Email can then be saved in a shared drive or some other means which enables it to be retained and shared as required by group members. The same process can be applied to meeting agenda and minutes.

3.1.3 Are email copies considered government records?

Email messages sent internally for administrative or organizational requirements through postmaster, departmental distribution lists and workgroups, are considered duplicate copies. These messages should be deleted once the information is no longer required. The originator is responsible to ensure that the original messages are retained if they constitute government records.

Replies to any of these emails, add to the information and, therefore, may constitute a new record. In such cases, the person who replies is an originator and must determine whether this new message is a government record and needs to be retained.

Email messages from sources external to Government of Newfoundland and Labrador, which are distributed solely for information or reference purposes and are not required to

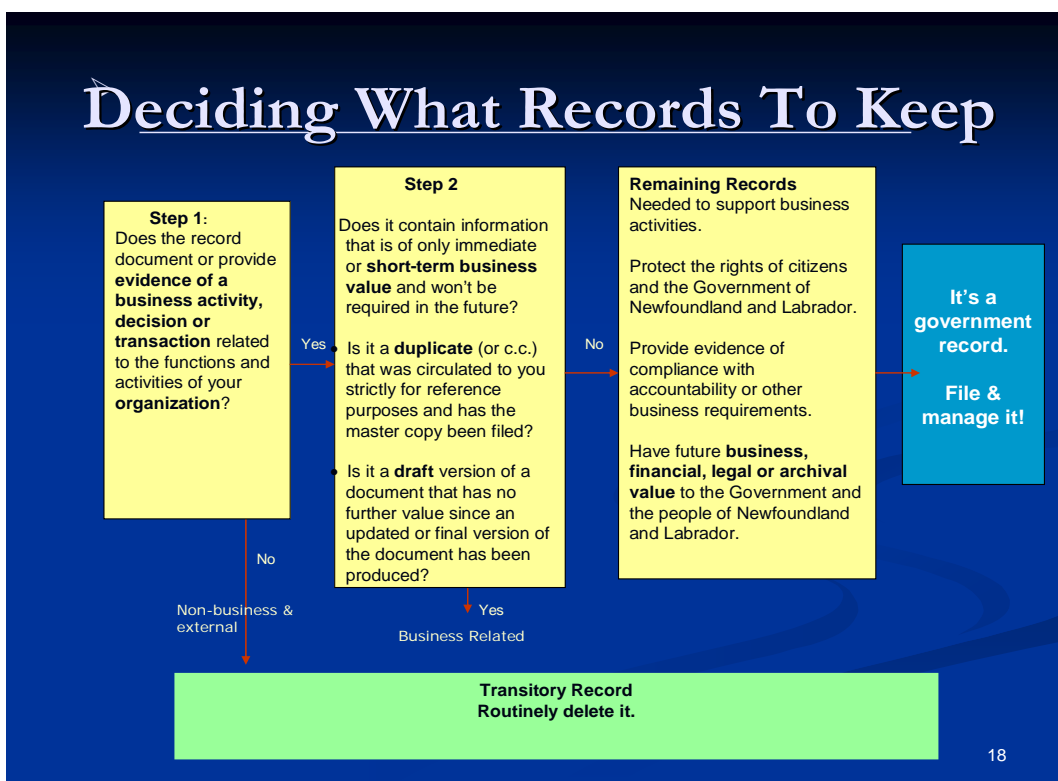
Government of Newfoundland and Labrador Email Guidelines

document the business of government, are not government records. These messages should be deleted once the information they contain is no longer required.

3.1.4 Which email messages are transitory records?

Transitory records are records required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record. Email transitory records are not required to control, support or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of the department. The diagram below can help to identify transitory records.

It may be useful to consider that some transitory email may be the sort of information one might share verbally, either in person or by phone, and not feel obliged to follow up in writing.



3.1.5 Backup and retention of email

Back-up measures have been established for Government of Newfoundland and Labrador email systems for disaster recovery purposes. These measures permit information to be restored should the system crash or the email system be damaged in some other way.

These procedures provide emergency back-up for server based mail systems and are **not** an email archive from which users can routinely restore accidentally deleted emails.

3.2 How do I file email?

Key concerns when filing email messages and attachments will be the ability to identify, retrieve and share this information, as required. If a user has established that an email message is a government record it must be managed and retained appropriately.

It is not recommended to keep an email record in more than one format. If it has been printed and filed, the electronic copy should be deleted. If the email has been filed in an Electronic Document Management System (EDMS), such as a TRIM system or shared directory, the copy in the email in-box should be deleted.

3.2.1 What is an Electronic Document Management System (EDMS)?

An Electronic Document Management System (EDMS) captures and stores electronic documents (including email messages) in a central repository. It allows users to assign information about records (metadata), such as a document title, subject, description and access rights. As well, an EDMS also automatically assigns such information as name and organization of the person filing the record, the document application type, etc. Authorized users can then research and retrieve documents based on the metadata entered in the system, or by using full-text searches.

An EDMS provides greater control for the management, identification and retention of an organization's electronic documents. It allows for the life-cycle management of this information in electronic format and facilitates the sharing of this information with broader audiences.

A government-wide initiative is under way to configure TRIM and implement it throughout Government of Newfoundland and Labrador with standard configuration, classification and practices. TRIM, along with the standard classification plan being developed by the Office of the Chief Information Officer will address document naming conventions, version control, authentication, workflow, records classification, security, and records disposition according to approved records retention and disposition schedules. TRIM can also handle the management of paper records with file folder and box level information.

Until TRIM is in place across government, departments and users must use existing technology to manage email records and other electronic records. Each department will have to examine the advantages and disadvantages of each approach for different groups of records and employ the approach which works best in their environment. The Office of the Chief Information Officer can provide advice through its Information Management Branch.

3.2.2 Records offices and hard copy files

In departments where there is no EDMS, it is advisable to print email government records for filing.

3.3 When can I destroy email messages?

It is illegal to destroy government records without authorization of the Government Records Committee, as established by *The Management of Information Act*. This

Government of Newfoundland and Labrador Email Guidelines

ensures a proper legal framework around the disposal of government records and facilitates the identification and preservation of archival and historical records.

3.3.1 When can I get rid of email government records?

As with any departmental record, email records, depending on their individual function and content, have varying retention periods. Retention can range from very short to long term according to the need for the record. Therefore, it is impossible to apply a universal rule to delete all email messages after a set period.

Departmental records can only be disposed of after legal authorization. These authorities include the Government Records Committee approval to dispose of records and the The Rooms, Provincial Archives subsequent decision on the form of disposition (either destroy records or transfer them to the The Rooms, Provincial Archives). While generic disposition authorities exist for administrative records (IMSAR) there is no standard authority for operational records.

Disposition authorities currently used for departmental records can be applied to either paper or email records maintained in electronic format. These authorities specify the approved retention periods. They should be applied only under the guidance of personnel trained in information management.

3.3.2 When can I destroy email transitory records?

Email messages determined to be transitory in nature (for definition of transitory records see section 3.1.4) should be regularly deleted once they are no longer of use to the email creator or recipient.

The only exception is if a department has already received a formal request under the *Access to Information and Protection of Privacy* legislation or is involved in a legal discovery process – **no email should be deleted if it is required for these reasons.**

3.3.3 Deleting email

Empty the “deleted items” folder regularly. Users should do regular clean-ups of their email in-box and “sent items” folder by filing email government records and by deleting the transitory emails. Refer to Section 2, Management of Email Messages. Regular clean-ups will prevent receipt of “mailbox full” messages, and will enable users to find and share information faster.

3.4 Responsibilities of departing/moving employees

Departing employees are responsible for ensuring that their email government records and their mailboxes are in order before their departure. Departing employees must save and file all those messages determined to be government records, as per the Email Policy and the guidelines outlined in this document. One or more of the following options may be employed:

- saving email government records to TRIM (preferred option where TRIM is available);

Government of Newfoundland and Labrador Email Guidelines

- filing email government records in electronic format within a shared directory in the appropriate directory files (if using a shared directory);
- with their manager's approval, assigning responsibility for an email account to another person with the understanding that this person will not delete email government records of the departing employee; and
- printing and filing email government records in the applicable records office or other applicable filing area. This would be appropriate in situations of a temporary nature such as maternity leave, secondment, etc.

Departing employees should delete all those messages that are not government records. If an employee is merely transferring within a department or departing for a temporary period of time and retaining his/her current email account, he/she may wish to keep his/her emails.

3.4.1 Managers' Responsibility

Before conducting the clean-up of email messages, a departing employee should consult with his/her supervisor to determine and agree upon the filing method for email government records. Managers are responsible to ensure that email government records, as well as those identified in Section 1.2, remain within the department. They are also responsible for ensuring that these email records are identified and filed so that they can be researched and retrieved, as required.

3.4.2 Removal of email accounts

When an employee is departing; the relevant Human Resources Division will inform the Office of the Chief Information Officer. The Office of the Chief Information Officer will remove the email account from the mail system after receiving confirmation from the departing employee's manager that no government records are stored in the email account. All records retained in the email account will be permanently deleted.

3.4.3 Abandoned Email Disposal Process

The *Management of Information Act* defines an abandoned record as:

“a government record to which ownership cannot be established and which has been determined to be an abandoned record by the chief information officer..”

A process for disposing of email accounts that contain abandoned records has been designed to accommodate exception to the regular management processes. It is expected that managers will ensure that departing employees will ensure that all government records are appropriately classified and filed in the departmental records management system. The need to manage abandoned email should therefore be limited.

In the event that an email account is abandoned the Office of the Chief Information Officer (cooperation between the IT and IM divisions) will undertake the following steps to facilitate disposal of the records in the account:

- Identify the name(s) on the account;
- Submit the name(s) to the Deputy Minister requesting sign-off for archival appraisal and disposal of records;
- Departments will be required to provide some additional information on the owners of the email boxes including position title, division/branch, and identification of current email filing guidelines (if available) in the Department;
- The Chief Information officer of the Office of the Chief Information Officer will authorize the designation of the email account as abandoned.
- The Rooms Provincial Archives government records archivist will complete a functional macro level appraisal by account;
- Accounts to be destroyed will be submitted to the Government Records Committee for official sign-off and deleted from mail servers;
- Accounts to be archived will be stored on off-line storage for the retention time identified by the Rooms Provincial Archives (actual process to be determined in consultation with the Office of the Chief Information Officer and the Provincial Archives); and

4.0 Creating and using email

4.1 How to use email effectively

Email provides an ideal tool to quickly and easily communicate and share information. It allows users to send information to one or several recipients simultaneously, offering greater opportunities for productivity. Each user is responsible to implement practices to reduce the “clutter” or volume of email traffic on a system including:

4.1.1 Misuse of email

Users can easily fall into the trap of forwarding chain letters or SPAM to other users. These types of messages are frequently hoaxes that entice or may even insist that recipients forward them on. Recipients of an email SPAM or chain letter should not forward or reply to it. Recipients are responsible for this email and should delete it immediately from their mailboxes.

The government has anti SPAM filters in place to try to prevent SPAM from entering the government email system. The process for determining SPAM is not one hundred (100) per cent accurate, what is SPAM or junk mail to one person may be a legitimate piece of mail for another.

To prevent legitimate email from being stopped, the addresses of known legitimate senders can be placed on a “safe” list so that mail from these sources will be delivered. In cases where a user feels her/his legitimate mail may be being caught by SPAM filters, he/she should contact the Office of the Chief Information Officer Helpdesk concerning adding addresses to the exclusion list.

4.2 Who owns email on the Government of Newfoundland and Labrador system?

Email messages created in the conduct of government business are the property of the Government of Newfoundland and Labrador. They may be accessed by government personnel who are authorized to do so and have an appropriate reason for access.

4.3 What legislation applies to email?

Email messages, identified as government records, are subject to the same legislation and policies as other government records. These include, for example: the *Management of Information Act*, the *Access to Information and Protection of Privacy Act*, the *Evidence Act*, the *Electronic Commerce Act* and the discovery of evidence rules in the Rules of Court.

4.4 Legal issues

Email messages may be evidence in legal proceedings. Rules of disclosure are the same as for paper records. This means that organizations can be required to provide their email messages in legal proceedings.

Government of Newfoundland and Labrador Email Guidelines

Email must be used in compliance with Canadian and Newfoundland and Labrador laws and regulations. Activities such as disseminating messages that promote hatred against identifiable groups or an individual, distributing obscene material, or violating another person's copyright, are unlawful.

4.5 Can anyone gain access to a user's email?

Email created or received in the conduct of departmental business must be accessible for business-related purposes, and meet legislative and departmental accountability requirements. This underscores the need for the regular maintenance, organization and filing of email government records, and the deletion of non-government record material.

With the exception of email covered by specific exemptions the public can gain access to email messages under the *Access to Information and Protection of Privacy Act*.

4.5.1 Monitoring of email

To mitigate any security concerns, and to ensure that email is not misused, the Government of Newfoundland and Labrador shall monitor email traffic and content for viruses and SPAM, so that problems can be investigated.

The Government of Newfoundland and Labrador scans all email messages that pass through its infrastructure to check for computer viruses, worms or other malicious items that could pose a threat to the security of the Government of Newfoundland and Labrador network. All efforts will be made not to transport questionable email to and from the user. For additional details on email monitoring practices of the Government of Newfoundland and Labrador please contact the Office of the Chief Information Officer Help Desk.

Access to email by system administrators

System Administrators may be required to access email accounts. This will be done only in limited circumstances, such as:

- with a user's permission, to rectify a problem;
- by a Deputy Minister (or delegate), to access a specific business-related email. This would occur in a situation when the user is away from the office or unavailable and where the email is otherwise inaccessible and is required immediately. The user will be notified by Human Resources or her/his Deputy Minister (or delegate) of this action; and
- to investigate suspected misuse of email.

Collection, use and disclosure of personal information of employees, citizens or clients involving an email system will be done in accordance with the legal requirements of the *Access to Information and Protection of Privacy Act* to investigate suspected misuse of email.

Government of Newfoundland and Labrador Email Guidelines**4.5.2 Email system audit trails**

System audit trails automatically record the circumstances surrounding log-in attempts, creation, transmission and receipt, filing and retrieval, updates and deletion of messages in an email system or on a network. The Government of Newfoundland and Labrador maintains email system audit trails.

4.6 Privacy

Users should seriously consider privacy and confidentiality when choosing email as a means of communication.

Choosing email to communicate personal information about a third party or a user's own personal information, or to send information that is security classified, considerably increases the likelihood of unauthorized disclosure. Email messages could be intercepted in transit or be read by someone else. It is also important for users to remember that email messages can easily be forwarded to others, or even accidentally sent to the wrong address.

4.7 Security

The Government of Newfoundland and Labrador does not currently have enabled security features with the ability to digitally sign and/or encrypt email messages and attachments. Without such protection, information transmitted electronically can be easily compromised by casual eavesdropping at message storage points or by deliberate monitoring of the circuit. A key concern about system integrity is the possibility that an email message may never reach its intended recipient and the sender may be unaware of that fact.

Users should always use email with the assumption that messages may be read by someone other than the intended recipient. Think of email as an electronic postcard. It is not in an envelope and any system that it passes through has the potential ability to read its contents. Users should write email records with the same professional standard they would apply to creating paper records.

By the very nature of the internet, once an email message leaves the Government of Newfoundland and Labrador network, there is no control over what systems it passes through en route to the intended recipient.

4.7.1 Security of Attachments

Attachments are a serious security threat because of their potential for damage. They can automatically scan the user's address book and send an infected message to the addresses. As well, viruses can be attached to any type of file. The majority of users open attachments without question, or even have their software open attachments automatically upon receipt. Users are advised to:

- Avoid opening suspicious attachments, regardless of the sender;
- Check with the sender about the authenticity of an attachment before opening it; and

Government of Newfoundland and Labrador Email Guidelines

- Turn off the email function that automatically opens attachments.

5.0 References

5.1 Relevant Legislation

The management of Government information exists within a legislative framework that spans several departments and types of functions and authorities, including individual departments, the Office of the Chief Information Officer, the Provincial Archives, the Government Records Committee, the Office of the Access to Information and Protection of Privacy Coordinator, Information Technology and Information Management Personnel and individual public employees.

Management of Information Act - <http://www.hoa.gov.nl.ca/hoa/statutes/m01-01.htm>

Rooms Act - <http://www.hoa.gov.nl.ca/hoa/statutes/r15-1.htm>

Access to Information and Protection of Privacy Act - <http://www.hoa.gov.nl.ca/hoa/statutes/a01-1.htm>

Transparency and Accountability Act - <http://www.hoa.gov.nl.ca/hoa/statutes/t08-1.htm>

Evidence Act - <http://www.hoa.gov.nl.ca/HOA/statutes/e16.htm>

Electronic Commerce Act - <http://www.hoa.gov.nl.ca/hoa/statutes/e05-2.htm>

Financial Administration Act - <http://www.hoa.gov.nl.ca/hoa/statutes/f08.htm>

5.2 Policies

- Blackberry Usage Policy
- IT Security Framework – under development
- Email Policy - http://www.ocio.gov.nl.ca/im/policies/email/email_policy.pdf
- Access to Information and Protection of Privacy Act Policy and Procedures – under development

6.0 Key Contacts

- IM Branch, Office of the Chief Information Officer
 - im@gov.nl.ca
 - 729-0227
- The Rooms Provincial Archives
 - archives@therooms.ca
 - 757-8030
- Office of the ATIPP Coordinator
 - 729-7939
- Office of the Chief Information Officer Help Desk
 - 729-4357 or servicedesk@gov.nl.ca

Appendix 1 – Glossary and Terms

- [Abandoned Record](#)
- [Active Record](#)
- [Administrative Records](#)
- [Archival Appraisal](#)
- [Authenticity](#)
- [Back-up](#)
- [Classification Plan \(file\)](#)
- [Data Conversion](#)
- [Data Migration](#)
- [Destruction](#)
- [Disposal](#)
- [Disposition](#)
- [Electronic Document Management System \(EDMS\)](#)
- [Email](#)
- [Encryption](#)
- [Government Record](#)
- [Government Records Committee \(GRC\)](#)
- [Information Management System for Administrative Records \(IMSAR\)](#)
- [Integrity](#)
- [Inventory](#)
- [Life Cycle](#)
- [Metadata](#)
- [Office of Primary Responsibility \(OPR\)](#)
- [Operational Records](#)
- [Records Management System](#)
- [Records Retention and Disposal Schedule](#)
- [Reliability](#)
- [Semi-active Records](#)
- [SPAM](#)
- [Structured Record](#)
- [Transitory Record](#)
- [TRIM](#)
- [Unstructured Record](#)
- [Usability](#)
- [Vital Record](#)

Government of Newfoundland and Labrador Email Guidelines

Abandoned Record - An abandoned record is a [government record](#) to which ownership cannot be established and which has been determined to be an abandoned record by the Chief Information Officer (CIO) of the Office of the Chief Information Officer (OCIO).

Active Record - A record which is regularly referenced or required for current use (also called a current record). These records are usually kept within the primary office space or in a records centre or registry.

Administrative Records - Administrative records are required by all organizations to function. These “lights on” records document administrative processes including human resources, general administration, facilities management, financial management, information and information technology management, and equipment and supplies (material) management. Because the value of these records is consistent across Government Departments, the OCIO maintains the [Information Management System for Administrative Records \(IMSAR\)](#) as a standard for their management.

Archival Appraisal - Archival appraisal is the process of determining the long term value of records after they have completed the primary purpose(s) for which they were created. Approximately 95% of all records created have no archival value and should be destroyed at the end of their [life cycle](#).

Authenticity – Authenticity verifies that a record has not been modified or corrupted following creation, receipt, [migration](#) or [conversion](#).

Back-up – A Back-up is a copy of a record that is any of the following:

- Additional resource or duplicate copy on different storage media stored offline for emergency purposes
- Disk, tape or other machine readable copy of a data or program file
- Data or program file recorded and stored offline for emergency or archival purposes
- Record that preserves the evidence and information it contains if the original is not available

Classification Plan: A classification plan is the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules and represented in a classification system.

Data Conversion – Process of changing records from one medium to another or from one format to another.

Data Migration – Data Migration is moving sets of recorded information from one Information Technology System or device to another, as required by changes in a system configuration or requested by a user, while assuring that the data will be addressable and that data integrity will be maintained in the new environment.

Destruction - The physical destruction of records that are deemed to have no archival value.

Disposal – Disposal in the context of a records retention schedule, disposal can mean either destruction of records or transfer to archives for permanent retention. It is the final stage of the records [life cycle](#) or continuum.

Disposition - In the context of a records retention schedule, disposition can mean either destruction of records or transfer to archives for permanent retention. It is the final stage of the record's [life-cycle](#).

Government of Newfoundland and Labrador Email Guidelines

Electronic Document Management System (EDMS): An EDMS is a software package which provides tools for storing and managing unstructured electronic records. [TRIM](#) is an example of an EDMS.

Email: Email is defined as messages, including attachments sent and received electronically between personal computers or terminals linked by communications facilities. This includes address information (to, from, cc, bc, subject and date) and the message content.

Encryption – Encryption is the operation by which plain text is modified with an intelligible, non-exploitable text making it non-retrievable except by authorized users that have the key to bring it back to its original form.

Government Record - A Government Record is a record created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and an abandoned record. Disposal of a government record must be sanctioned by a records retention and disposal schedule that has been approved by the [Government Records Committee \(GRC\)](#).

Government Records Committee (GRC) – the GRC is the official body that is mandated to:

- Review and revise schedules for the retention, disposal, destruction or transfer of government records.
- Make recommendations to the minister respecting public records to be forwarded to The Rooms, Provincial Archives.
- Authorize [disposal](#) and [destruction](#) standards and guidelines for the lawful disposal and destruction of public records.
- Make recommendations to the minister regarding the removal, disposal and destruction of records.

Information Management System for Administrative Records (IMSAR) – IMSAR is provides a records retention and disposal schedule for administrative records that can be used by all government departments.

Integrity - Integrity demonstrates that the record is complete and has been unaltered.

Inventory – And Inventory is a detailed survey of the organization's records, including descriptions, scope, volume, frequency of use, method of organization and retention periods. It is used as the basis for developing a records management system.

Life Cycle – The life cycle refers to the stages through which information is managed. Information management strives to manage the records in a manner that facilitates [authenticity](#), [reliability](#), [integrity](#) and [usability](#) throughout all stages including:

- Planning
- Creation and organization
- Receipt and capture of data
- Retrieval, processing, dissemination and distribution of data;
- Storage, maintenance and protection
- Archival preservation or destruction or expungement

Metadata – Metadata is data about data elements including data descriptions, data ownership, etc. Metadata provides the information required to manage records. The creation and end date, for example are key pieces of information required to implement a [records retention and disposal schedule](#).

Government of Newfoundland and Labrador Email Guidelines

Office of Primary Responsibility (OPR) – The OPR (also called Office of Record) is the office which creates or acquires the original of a record, and is responsible for maintaining it. Copies of the original which may exist in other offices generally have shorter retention periods than the original in the OPR.

Operational Records - Operational Records are records which are unique to the mandate of their creators. Unlike [administrative records](#), these will be different in each organization. Each Department is responsible for the development, implementation and maintenance of records retention and disposal schedules for the operational records that they generate/receive.

Records Management System: An information system primarily designed to assist an organization in managing its recorded information concerning its recordkeeping practices from inception to disposition of records.

Records Retention and Disposal Schedule: A records retention and disposal schedule is a legal document that guides the management of a government record.

- Define the content of the record series or types.
- Link the records to the organizational unit and business process
- Dictate how long the records need to be retained in [active](#) and [semi-active](#) storage to meet operational and legislative requirements
- Authorizing the [disposition](#) of information in a legal manner.

Reliability – Reliability affirms that the content of a record is a trustworthy and a complete account of an activity or process.

Semi-active Records – Semi-Active records are those records that do not have to be readily available in primary offices but which still need to be kept for the possibility of use or reference. These records should be stored in appropriate storage facilities.

SPAM: Spam refers to electronic junk mail or junk newsgroup postings. It is defined in more general terms as any unsolicited email. In addition to being a nuisance, spam also eats up a lot of network bandwidth.

Structured Records - Structured records are defined as information stored in fields and rows in tables in a relational database. Structured records may constitute a [government records](#) when generated or received to complete government business transactions.

Transitory Record - A transitory record is a [government record](#) of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can be securely destroyed when no longer of value without a [records retention and disposal schedule](#).

TRIM: TRIM is the standard electronic document management system ([EDMS](#)) of the Government of Newfoundland and Labrador. Information about TRIM can be found at www.towersoft.com/na (LINK), or by contacting the Government of Newfoundland and Labrador TRIM Program Manager at 729-6723.

Usability - Usability refers to the ability to locate, retrieve, present and interpret records over time.

Government of Newfoundland and Labrador Email Guidelines

Unstructured Records - Unstructured records are defined as masses of information which do not have a data structure or one that is easily readable. Unstructured records are created via common desktop applications, such as Microsoft Outlook, Word and Excel, etc. to support ongoing business activity. An EDMS like [TRIM](#) is used to manage unstructured records.

Vital Record - Records necessary to continue the operation of an organization in case of emergency or disaster.



Government of Newfoundland and Labrador
Office of the Chief Information Officer

GUIDELINE – DISCOVERY AND LEGAL HOLD

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2009-335** approved by Treasury Board on November 19, 2009. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Department	Office of the Chief Information Officer
Issuing Branch	Application and Information Management Services
Date Issued	2011 11 01
Date Reviewed	2017 05 23
Review Cycle	Every 3 years

Table of Contents

1.0 Overview.....	3
2.0 Scope.....	4
3.0 Recommended Approach.....	5
3.1 Introduction.....	5
3.2 Managing Electronic Records Discovery.....	6
3.3 The Legal Hold Process.....	6
3.3.1 Approach.....	6
3.3.2 The Major Steps of a Legal Hold Process	7
3.4 Roles and Responsibilities.....	9
4.0 Glossary and Acronyms.....	11
4.1 Glossary	11
4.2 Acronyms	11
5.0 References	12
6.0 Revision History	13
Appendices	14
Appendix A: Major Steps in the Legal Hold Process	15

1.0 Overview

The Discovery and Legal Hold Guideline (hereafter referred to as the Guideline) is an OCIO Guideline on the measures required to support legal hold and the discovery process.

The purpose of the Guideline is:

- to ensure that departments understand and support the discovery process and requirements created by litigation,
- to ensure that departments are aware of their legal hold obligation, which includes the duty to preserve relevant information whenever litigation is reasonably anticipated, threatened or pending, and
- to provide practical guidance on how a department should fulfill obligations with respect to the preservation and production of relevant documents for legal hold.

IM Services (OCIO) uses the definition below when developing IM guidelines for use by public bodies.

Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

2.0 Scope

The Guideline is targeted to departments of the Government of Newfoundland and Labrador but may be adopted by all public bodies as defined in the Management of Information Act (*MOIA*), as deemed appropriate. Its audience includes Executive, senior management, legal counsel, and Information Management staff.

The Guideline outlines the steps necessary to effectively manage legal hold and discovery by providing information regarding the discovery and the legal hold processes.

The Appendices outline the major steps in the legal hold process.

3.0 Recommended Approach

3.1 Introduction

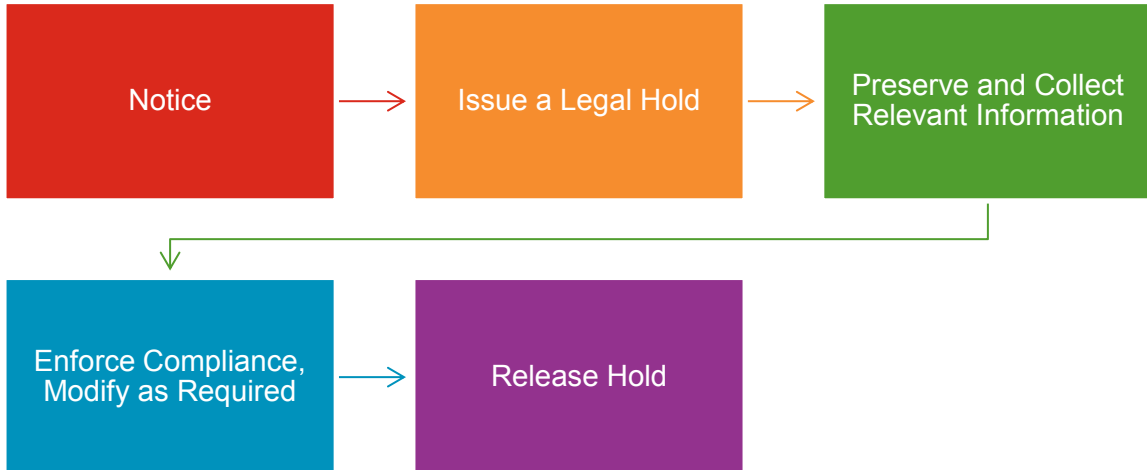
Records in all formats may be subject to legal hold and discovery requirements. Electronic records present particular challenges in terms of the potential volume of records, varying formats and ease with which they may be altered. The preservation, retrieval, exchange and production of documents from electronic sources in electronic form are referred to as “e-discovery.”

There is a need to ensure that information is protected, preserved and produced for litigation in the most efficient manner. Any public body that may reasonably expect that it may be the subject of litigation should, first and foremost, pay attention to proactive Information Management. This includes organization of information for ready access to serve on-going business, as well as retention and disposal schedules. In a litigation situation, a solid Information Management program facilitates a quick and uniform response to requests from legal counsel.

During the discovery phase of litigation, parties to a dispute must take appropriate, reasonable steps to locate relevant, responsive records in all formats in response to discovery requests.

3.2 Managing Electronic Records Discovery

E-discovery is the legal obligation of organizations to produce electronically stored information that is, or may be relevant to the subject matter of litigation. At a high level, e-discovery involves the following simplified process:



The key to successful e-discovery is the proactive and effective management of information in electronic form across multiple storage media and locations.

Spoliation: Spoliation can be defined as unauthorized destruction or alteration of a record. Electronic documents are easily deleted, either accidentally or in the normal course of business. Once litigation has commenced, there is an obligation to preserve documents. It is best practice however, for a party to preserve all potentially relevant documents as soon as it is reasonable to assume that litigation may ensue from an on-going issue. In this way, the party may avoid the appearance or allegation of spoliation.

3.3 The Legal Hold Process

Organizations have a duty to preserve relevant information whenever litigation is reasonably anticipated, threatened or pending. This duty arises regardless of whether the organization is the initiator or the target of litigation.

3.3.1 Approach

This section outlines a legal hold approach that departments can follow in the event of litigation. During an e-discovery process, all types of data may serve as evidence, such as e-mail, images, calendar files, databases, audio files, spreadsheets, HPRM files, animation, Web sites and computer programs. In general practice, e-mail is usually the most valuable source of evidence in civil litigation.

Once a legal hold is triggered there is a duty to preserve records which are deemed to be relevant to supporting the litigation. The duty to preserve supersedes Information Management policies or records retention and disposal schedules that would otherwise result in the destruction of records (including electronic records). The organization must take the necessary steps to implement the hold and suspend the disposal of all records in all formats which may be deemed to be relevant.

Legal Hold versus Access to Information (ATIPP) Request Process

It should be noted that while the legal hold process, like the ATIPP request process, requires the suspension of regular and normal disposal of records, the two processes are completely separate and should be treated as such. Departments are advised to consult their legal counsel if they have questions regarding any details or requirements of the legal hold process which are not outlined in this Guideline.

3.3.2 The Major Steps of a Legal Hold Process

Step 1: Notice

As a first step, departments need to be aware of the following types of triggers that often instigate the need to implement a legal hold:

- A preservation letter is issued to the department from an opposing counsel or the Department of Justice;
- A claim letter that is likely to lead to litigation or a statement of claim is filed either directly with a department or with the Department of Justice;
- A reasonable threat of litigation exists, for example, when dismissal of an employee is likely to result in a claim of wrongful dismissal.

Step 2: Issue a Legal Hold

Upon receipt of a Statement of Claim, and notification of legal counsel, the Department of Justice will issue a legal hold letter to the department. In such instances, the Deputy Minister or designate should issue a legal hold notice to relevant officials within the department, which is an instruction to preserve records and information that could be relevant.

Communicating with the Office of the Chief Information Officer (OCIO) as early as possible in the process is critical. Departments that are party to litigation must

ensure that relevant electronic records are preserved and protected against alteration or destruction.

Implementation of records disposal, including that authorized through records retention and disposal schedules, should be suspended until the legal hold is lifted. It may also be necessary, in collaboration with OCIO, to copy hard drive(s) and removable drives of some staff, as well as e-mail and other relevant electronic records.

Step 3: Preserve and Collect Relevant Information

It is best practice for a party to preserve all relevant documents as soon as possible. However, to avoid unnecessary retention of records in contravention of approved records retention and disposal schedules, a legal hold should be limited in scope to only those records deemed through advice from legal counsel to be relevant to the litigation.

Parties should agree as early as possible in the litigation process on the format in which electronically stored information will be produced. In general, production of electronic documents and data should be made only in electronic format, unless the volume of documents to be produced is minimal.

The practice of producing electronically stored information in paper format should be discouraged in most circumstances; paper is not searchable, is more time consuming to print and collate, and increases the cost of reproduction, shipping and storage; whereas multiple electronic copies can be made at a nominal cost.

Step 4: Enforce Compliance, Modify as Required

A department should always retain a copy of any legal hold notice(s) that have been issued, and a distribution list for the notice(s). Throughout the legal hold process, there should be continuous enforcement to ensure that parties are in compliance with the terms of the legal hold notice. The legal hold should be reviewed periodically, and modified if required.

Step 5: Release Hold

When the legal hold is no longer required, it should be released and Information Management processes, including authorized disposal of records, should return to normal. This should be adequately communicated at that time.

3.4 Roles and Responsibilities

Legal Counsel Responsibilities
<ul style="list-style-type: none">• Determine if circumstances merit the need for a legal hold• Determine the scope of the hold to be issued• Issue a legal hold notice to the Deputy Minister of the department• Identify the scope and collection method of the all records subject to the hold• Work with the department and OCIO to retrieve electronic records so that they can be reviewed by legal counsel to determine if they are useful as evidence• Identify and segregate privileged information• Monitor the hold and modify it if required• Release the hold
Departmental Responsibilities – Deputy Minister or Designate(s)
<ul style="list-style-type: none">• Ensure that records that are subject to legal hold are protected from unauthorized access and/or alteration at all times during the hold• Review the hold, and acknowledge its receipt• Notify departmental Information Management to ensure all information sources are identified and disposal of potentially relevant records is suspended• Comply with any instructions accompanying the hold• Advise all relevant staff to suspend all destruction of electronic records related to the hold (e.g., deletion of e-mails, drafts of documents, etc.)• Contact legal counsel when needing access to a document or file containing electronically stored information that may be relevant to the hold• Request that relevant staff identify the location of all potentially responsive information• Provide relevant computers / devices (including personally-owned computers and mobile devices if requested)

Departmental Responsibilities - Information Management

- Suspend any retention policy or records retention and disposal schedule affected by the hold
- Identify any potential sources of relevant information in all formats
- Assist in departmental compliance
- Resume records retention policy or authorized disposal of records upon release of the hold

OCIO Responsibilities

- Work with the department and legal counsel to identify the scope of electronic records that must be preserved, the identification methods, collection processes, and searches
- Collect and preserve electronic records, if possible to do so without changing the nature of the information
- Collect and make the electronic records available in appropriate formats

4.0 Glossary and Acronyms

4.1 Glossary

A complete listing of terms can be found on the OCIO website - [Information Management \(IM\) and Information Protection \(IP\) Glossary of Terms](#).

4.2 Acronyms

Abbreviation	Description
ATIPP	Access to Information and Protection of Privacy
IM	Information Management
<i>MOIA</i>	<i>Management of Information Act</i>
OCIO	Office of the Chief Information Officer
ESI	Electronically stored information
HPRM	Hewlett Packard Records Manager (previously TRIM)

5.0 References

Below is a listing of references included with this document; hyperlinked to the published internet location.

[Information Management and Protection Policy, TBM 2009-335](#)

[Management of Information Act](#)

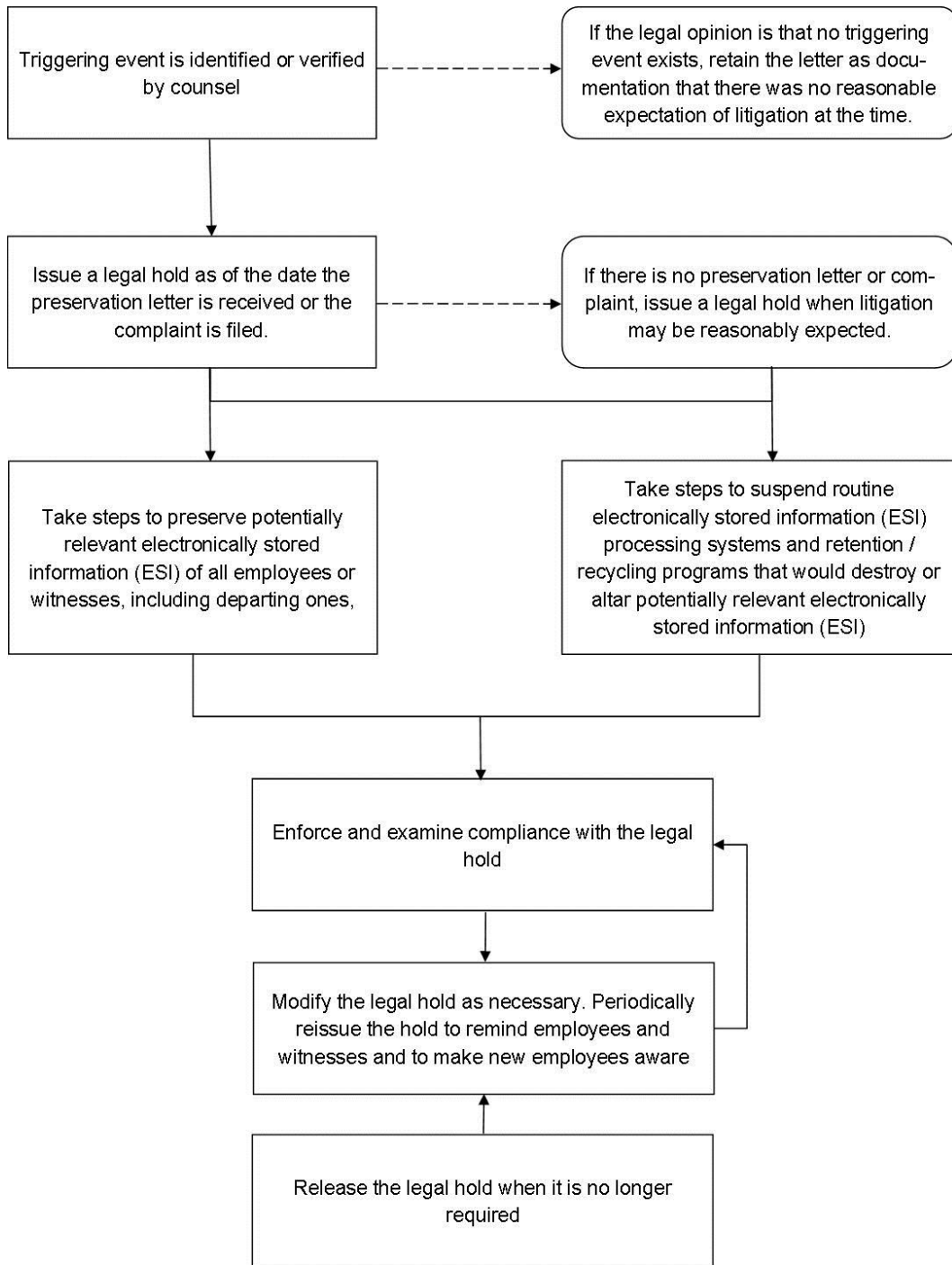
6.0 Revision History

Date (yyyy mmm dd)	Title or Group
2011 Jan 01	Executive Director, Information Management (OCIO)
2011 Jan 01	Legal Counsel (Justice)
2011 Jan 01	Assistant Deputy Minister, Courts and Related Services (Justice)
2011 Jan 01	Executive Director, Information Management (OCIO)
2011 Nov 01	Government Records Committee (GRC)
2017 May 11	IM Consultant, IM Advisory Services (OCIO)
2017 May 11	Director, Information Management Services (OCIO)
2017 May 23	Executive Director Application and Information Management Services (OCIO)

Appendices

Appendix	Title
A	Major Steps in the Legal Hold Process

Appendix A: Major Steps in the Legal Hold Process





Government of Newfoundland and Labrador
Office of the Chief Information Officer

GUIDELINE – MANAGING DEPARTMENTAL INFORMATION THROUGH THE EMPLOYMENT CYCLE

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2009-335** approved by Treasury Board on November 19, 2009. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Department	Office of the Chief Information Officer
Issuing Branch	Application and Information Management Services
Date Issued	2012-11-08
Date Reviewed	2017-05-23
Review Cycle	Every 3 years

Table of Contents

1.0 Overview3

2.0 Scope4

3.0 Background5

 3.1 *Management of Information Act*5

 3.2 *Access to Information and Protection of Privacy Act, 2015*.....5

 3.3 Risks Associated with Non-compliance5

 3.4 Office of the Chief Information Officer6

4.0 Recommended Approach7

 4.1 Employment Initiation7

 4.2 Transfer (Temporary to Permanent Status)9

 4.3 Transfer (New Position Inside the Department)10

 4.4 Leave of Absence10

 4.5 Transfer (New Position Outside the Department)11

 4.6 Temporary Assignment or Secondment (Outside the Department).....11

 4.7 Termination of Employment.....11

 4.7.1 Employee Initiated Termination.....11

 4.7.2 Employer Initiated Termination12

 4.7.3 Access to Personal Documents Following Termination.....13

5.0 Glossary and Acronyms14

 5.1 Glossary14

 5.2 Acronyms14

6.0 References.....15

7.0 Revision History16

Appendices17

 Appendix A: Employee Information Access and Asset Management Form18

1.0 Overview

All management-level employees have a responsibility to ensure that departmental information is managed properly through the employment cycle. The Government of Newfoundland and Labrador provides individuals with access to the information and Information Technology (IT) assets and services required to complete assigned work. While individuals must have timely access to information, it is equally important that their access is limited to what they need to perform assigned work. An individual may experience changes in their position or responsibilities that require modification to the information they access or maintain. This modification should be completed in a timely manner. Information no longer actively used by an individual should be transferred to the department's records management system or disposed of as per the *Management of Information Act (MOIA)*.

IM Services (OCIO) uses the definition below when developing IM guidelines for use by public bodies.

Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

2.0 Scope

This Guideline applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the Government of Newfoundland and Labrador (hereafter referred to as individuals).

3.0 Background

The *Management of Information Act* requires that departments manage and protect information. The *Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)* places limitations on how information can be collected, used and accessed. To support compliance with these legislative requirements, departments must ensure that employees are provided with access to appropriate information required to support their existing assigned duties. When an employee's role changes, management should consider whether the information to which the employee has access must be modified, transferred or discontinued.

3.1 *Management of Information Act*

The *Management of Information Act* (Section 6) requires that each department implement an Information Management (IM) program to facilitate the economical and efficient creation, maintenance, retrieval, protection and disposal of government records. It is important that all employees are made aware of their responsibilities for IM as they begin their employment with government. Employees should also ensure appropriate measures are taken to properly manage information when there are changes in their employment (e.g., transfer to another department, leave of absence). Information that is created or received by a department to support its mandated programs and services is the property of that department. It must be retained internally when an individual terminates employment to ensure proper management and disposal. Under the *Management of Information Act* it is unlawful to damage, mutilate or destroy a government record or remove or withhold a government record from the possession of a public body.

3.2 *Access to Information and Protection of Privacy Act, 2015*

The *Access to the Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)* dictates that while government is open and accountable to the public through access to information it collects and maintains, personal or confidential information required to support the delivery of public programs and services is protected from inappropriate access. This includes internal access to information by departmental employees. Each department is responsible for ensuring that requirements for *ATIPPA, 2015* are met for the information they create and maintain.

3.3 Risks Associated with Non-compliance

Risks that may be associated with poor management of information through the employment cycle include:

- Employees unaware of their IM responsibilities may put the department at risk of non-compliance with legal and regulatory requirements.

Guideline – Managing Departmental Information through the Employment Cycle

- Inappropriate access to information may occur if procedures for assigning and tracking access to information are not in place throughout the employment cycle.
- Employees may transfer within or from a department or terminate government employment in possession of or with on-going inappropriate access to departmental information; thereby risking compliance with the department's requirement to manage, protect and dispose of its own information.
- If departmental information is not retained and catalogued following the termination of employment there is a risk that ATIPP requests may not be processed comprehensively. Alternatively, departmental information that has been properly disposed of by a department may be discovered in the possession of an employee that no longer reports to the department.

3.4 Office of the Chief Information Officer

As the custodian of electronic information on behalf of government departments, the Office of the Chief Information Officer (OCIO) plays a critical role in ensuring appropriate access and retention of information. It is the responsibility of a department to communicate change requests related to employee access to information in a timely manner. This supports the ability of technical staff to initiate, modify and disable employee access to the Government IT Network within the appropriate timeline.

OCIO provides individuals with IT Services required to do their work. OCIO is made aware when an individual terminates employment through updates from the Payroll Division. At that time, the individual's IT Network Account is disabled and any remaining data is transferred to the departmental IM staff.

There are many scenarios in which an individual's employment status or reporting relationship within government may change in a manner that requires modification to their information access or IT services. OCIO is not notified automatically when employees change positions or transfer to another department. It is therefore critical that managers notify the OCIO of all required changes to information access.

4.0 Recommended Approach

Managers are strongly encouraged to implement the recommended approach described in this document to minimize the impact of departing employees and to ensure that departmental information is retained when employees transfer to another department.

The employment cycle refers to the stages through which an employee transitions through their career within the Government of Newfoundland and Labrador. Stages include:

- Employment Initiation
- Temporary Assignment or Secondment to another role
- Temporary to Permanent Status
- Transfer to a New Role
- Leave of Absence
- Termination

The approach described in this document is intended to augment existing departmental protocols where required. Identify and verify with departmental human resource representatives and IM staff any internal protocols that must be followed.

4.1 Employment Initiation

Employment initiation provides an opportunity to ensure each employee is provided with an understanding of their IM requirements and the departmental IM resources available to them. Individuals that are new to working with the Government of Newfoundland and Labrador participate in a mandatory onboarding program. The completion of **IM@Work**, OCIO's online course provides employees with an overview of government-wide IM requirements.

Additional departmental activities recommended include:

Prior to start date:

- Complete OCIO's form **Request for Network Accounts and/or Computer Equipment**, found on **OCIO Help**, to initiate OCIO services and equipment required by the individual. This form will require that you identify all access requirements including departmental file share, business applications, etc.

Guideline – Managing Departmental Information through the Employment Cycle

- Notify your IM staff that a new employee will be joining the department to ensure any departmental requirements or support is engaged.

Within the first Two Weeks of Employment:

- Create a listing of the information and technology assets allocated to the employee. A sample **Employee Information Access and Asset Management Form** is located in the Appendices.
- Departmental Records Management System (e.g. paper or electronic systems such as HPRM). Follow up with departmental IM staff to schedule required training.
- Review with the employee all required business processes. The following should be identified:
 - Forms and templates used to ensure that information gathered to support processes is consistent and appropriate. Ensure the employee knows where to find the most updated forms and templates and receives instruction on their use.
 - Access to any sensitive information and provide an explanation as to why the employee will require access. Use the requirements outlined in *ATIPPA, 2015* to identify sensitive information.
 - Appropriate policies, procedures or guidelines used to manage and protect information.
- Provide an overview of the department's IM program including locations, services, contacts, etc.
- Direct the employee to the **OCIO website** for more information on best practices for managing information.
- Outline any departmental IM policies, standards or guidelines related to IM by directing the employee to the IM staff and requesting an orientation.
- Provide orientation on how program areas organize and store their information including:
 - Paper and electronic records programs.
 - Departmental use of the Shared Drive.

Guideline – Managing Departmental Information through the Employment Cycle

- Departmental use of personal workspace on the network (P: Drive).
- Employees are directed not to use government IT assets for personal use in the Directive **Acceptable Use of the Government Network and Information Technology Assets**. It is expected that personal documents that support the employee's development and career management such as resumes, leave slips, learning and development resources, awards and certificates, etc. may be stored at the workplace. Managers are to advise all employees that this information should be clearly marked personal through storage in an electronic or paper folder titled "Personal." This is with the understanding that the government retains the right to access any information stored within its assets if required.

One to Three Months after Start Date:

- When an employee begins work the scope of their role within the program area may not be fully known. Follow up with the employee to verify that the above described steps have been completed (e.g., that all business processes have been explained, forms and templates have been provided, etc.).

4.2 Transfer (Temporary to Permanent Status)

Temporary status is defined as employment with reference to a specific date of termination of service.

- In this situation there may be a minimal impact on information access.
- Managers are advised to complete the attached appendix **Employee Information Access and Asset Management Form**, a sample can be found in the Appendices, when an individual begins employment to ensure that they have full access to the information and IT services required to fulfill assigned work duties.
- Notify OCIO IT Service Desk that the termination date previously identified for the employee is no longer valid.
- Update the **Employee Information Access and Asset Management Form**, a sample can be found in the Appendices, as required.
- Notify the employee that changes have been made. Provide instructions, support materials and contact information as required to support the use of any new resources.

4.3 Transfer (New Position Inside the Department)

Individuals may transfer to a new position within the department that differs from that which they had previously held.

- The impact in this situation will vary depending on the nature of the new role that the individual is moving to. If it is in the same program area there may be minimal impact.
 - Review and update the **Employee Information Access and Asset Management Form**, a sample can be found in the Appendices.
 - Submit a request to the OCIO Service Desk to modify access to business applications, departmental file share locations, etc. to which the employee no longer requires access and for new ones to which the employee may require access in their new role
 - Notify the employee that changes have been made. Provide instructions, support materials and contact information as required to support the use of any new resources.
- If the transfer is to another program area follow the steps described in Section 4.7 Termination of Employment of this guideline.

4.4 Leave of Absence

There are numerous circumstances under which an employee may be granted leave from their position for an extended period of time with the expectation that they will return to employment.

In this situation it is important that all information required to support ongoing operations in the employee's absence is transferred as appropriate to either another employee or to the department's records management system. Follow the steps described in Section 4.7.1 Employee Initiated Termination of this guideline.

OCIO provides individuals with IT Services required to complete their work. When employees do not login regularly to their IT network account there is a risk that inappropriate access may go undetected. OCIO must be informed that employee access to the government network must be suspended because of leave of absence and not termination of employment. In this instance OCIO will disable the account and transfer the data to the individual's manager or designate. This information can be restored to the user upon their return to work.

4.5 Transfer (New Position Outside the Department)

Departments are responsible for the management, retention, and disposal of departmental information. If an employee leaves a position to take another within Government they should no longer have access to departmental information, including electronic and paper records, email and departmental business applications. Follow the steps described in Section 4.7 Termination of Employment.

4.6 Temporary Assignment or Secondment (Outside the Department)

Temporary assignment or secondment to another position outside the department means that the employee continues to be employed by the department but will be working on behalf of another department within Government. Managers should assess information access requirements on a case by case basis. In some instances, an employee may be seconded to a project on behalf of a department and may be expected to bring departmental knowledge into the role. In this situation, it may be appropriate for the employee to retain access to departmental information. In most situations, the employee is seconded to a role completely independent of their home department. In this situation all access to departmental information should be discontinued following the procedures described in Section 4.7 Termination of Employment.

4.7 Termination of Employment

4.7.1 Employee Initiated Termination

Termination of employment occurs for many reasons. When an employee leaves government it is critical that the department retains its information so that it may be managed as required by the *Management of Information Act*. From an operational perspective, it is essential that information and resources are identified and transferred appropriately to ensure a continuation of the program and services the employee supports following their termination date. In most situations there is reasonable notice of the termination date. The following steps should be taken prior to termination:

- Review the **Employee Information Access and Asset Management Form**, a sample can be found in the Appendices, from when the employee began employment to identify the information to which they have been provided access.
- Submit a request to the OCIO Service Desk to modify access to business applications, departmental file share locations, electronic content management systems such as HPRM to which the employee no longer requires access following termination date.
- Advise the employee that they are responsible for the removal of all personal records stored on the government IT network, P:drive, email and in hard copy. This includes leave slips, resumes that do not reflect departmental business but

Guideline – Managing Departmental Information through the Employment Cycle

may have been retained by the employee at work for convenience. This information should be transferred to a portable storage device or CD prior to departure.

- Meet with the employee prior to departure to review the information that is in their possession to identify required activities including:
 - Secure disposal of transitory records.
 - Transfer and/or disposal of government records as per departmental Records Retention and Disposal Schedules.
 - Transfer of records to the departmental records management system.
 - Identify staff to whom information must be transferred prior to departure.
 - Provide IM support contact information.
- Request that the employee transfer any information in their position to either the manager, designate or IM staff. Note all information should be sorted, classified and organized according to departmental classification standard. This includes:
 - Notifying the departmental Electronic Content Manager (e.g. HPRM administrator) of the employee's termination date to ensure access is disabled
 - Forward the **Employee Information Access and Asset Management Form**, a sample can be found in the Appendices, to the IM staff within your department. This will assist them in processing any future information requests receive by the department involving the employee.

4.7.2 Employer Initiated Termination

The majority of terminations are initiated by the employee due to things like retirement or simply a move to another opportunity. In such situations, planning with the employee on how to transfer information is achievable. In the event that a termination is initiated by the employer it is important to work with legal, human resource, departmental and OCIO contacts prior to notifying the employee of the termination to ensure that information in their custody is identified and protected.

- Review the **Employee Information Access and Asset Management Form**, a sample can be found in the Appendices, to identify the nature of the information that is maintained by the employee.

Guideline – Managing Departmental Information through the Employment Cycle

- Work with departmental IM staff to properly manage departmental information that had been in the employee's custody prior to termination.
- Identify the location of all physical records maintained by the employee. This is especially important if the employee may have departmental information stored at an alternate location (e.g. home office) or if the employee has possession of unique records that cannot be reproduced.
- Before notifying the individual of their termination you should notify OCIO as soon as the termination date has been identified. This will enable OCIO to create a snapshot of the electronic information maintained by the employee prior to notification. It is imperative that any requirements for the restoration of information are identified as soon as possible.

4.7.3 Access to Personal Documents Following Termination

Departmental information that is maintained by an employee must be retained by the department prior to termination. Following the termination of an employee, OCIO's procedure is to transfer data stored in an employee's IT Network Account including email and P: Drive contents to departmental IM staff for either disposal or incorporation into the department's records management system.

In the event that personal documents are stored either in paper or electronic format it is the responsibility of the department to process a request from the employee to gain access to this information. Recommended steps include:

- Verify the department's procedures with HR and IM staff.
- Obtain the request from the individual in writing including detailed description of the content and location of information (e.g., email in an inbox folder titled "personal").
- Validate the information in question is of a personal nature (e.g. copies of leave slips, resumes, photos, etc.) and not used to support departmental business activities (e.g. business contacts acquired during employment).
- In the event that personal information coexists with departmental information the departmental information should be severed from the content in the same manner as an ATIPP request is processed.
- Obtain Executive approval for the release of the information.

5.0 Glossary and Acronyms

5.1 Glossary

A complete listing of terms can be found on the OCIO website - [Information Management \(IM\) and Information Protection \(IP\) Glossary of Terms](#).

5.2 Acronyms

Abbreviation	Description
ATIPP	Access to Information and Protection of Privacy
<i>ATIPPA, 2015</i>	<i>Access to Information and Protection of Privacy Act, 2015</i>
HPRM	Hewlett Packard Records Manager (previously TRIM)
HR	Human Resources
IM	Information Management
IP	Information Protection
<i>MOIA</i>	<i>Management of Information Act</i>
OCIO	Office of the Chief Information Officer

6.0 References

Below is a listing of references included with this document; hyperlinked to the published internet location.

[Acceptable Use of the Government Network and Information Technology Assets](#)

[Access to Information and Protection of Privacy Act, 2015](#)

[Employee Orientation Program: Guidelines For Effective New Employee Orientation](#)

[Human Resource Policies](#)

[IM@Work \(PSAccess\)](#)

[Information Management and Protection Policy, TBM 2009-335](#)

[Management of Information Act](#)

[OCIO Help \(internal account access only\)](#)

[OCIO website](#)

[Request for Network Accounts and/or Computer Equipment Form](#)

7.0 Revision History

Date (yyyy mmm dd)	Title or Group
2011 Dec 15	IM Consultant, IM Advisory Services (OCIO)
2011 Dec 15	IM Consultant, Government Records Lifecycle Management (OCIO)
2011 Dec 15	Director, Information Management Services (OCIO)
2012 Jan 11	Executive Director, Information Management (OCIO)
2011 Feb 14	Information Management Standards Board (IMSB)
2012 Mar 12	Information Management Directors Forum
2017 Apr 10	IM Consultant, IM Advisory Services (OCIO)
2017 May 11	Director, Information Management Services (OCIO)
2017 May 23	Executive Director Application and Information Management Services (OCIO)

Appendices

Appendix	Title
A	Employee Information Access and Asset Management Form

Appendix A: Employee Information Access and Asset Management Form

Employee Information Access and Asset Management Form

The information on this form is collected for the purpose of tracking the use of departmental informaiton assests.

Departmental Information			
Employee Name			
Employee Title			
Primary WorkLocation			
Manager Name			
Manager Contact Information			
Desription	Requirements	Review Date	Initial
Date of Hire	<i>Date on which employee begins work</i>		
Date of Termination	<i>Date on which employee finishes work</i>		
IT Network Account			
Request Form Submitted	<i>Required to create a new IT Network Account. Submit request form 2 weeks prior to date of hire</i>		
Laptop/desktop computer Issued	<i>Indicate whether employee received a laptop or desktop</i>		
Departmental File Share Access	<i>List all departmental file share storage locations that the employee is provided access</i>		
Business Applications	<i>List all business applications to which the employee is provided access. Also note type of access (user, administrator, power user, etc.)</i>		
HPRM Access requested	<i>Follow departmental procedures for access to the departmental HPRM system. Indicate type of access provided.</i>		
Keys	<i>List identification numbers for departmental keys provided to the employee including individual rooms, storage areas, filing cabinets, etc.</i>		
Portable Storage Device	<i>Identify any portable storage devices provided to the employee with identification numbers (if applicable)</i>		

MANAGING THE RECORDS OF EXTERNAL PUBLIC BODIES

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Application and Information Management Services
Date Issued	2018-01-16
Review Date	As required.

APPROVAL AND SIGN OFF

Executive Director, Issuing Branch	Julie Moore, Application and Information Management Services
	January 16, 2018

Note: Questions related to this policy should be forwarded to OCIO@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	2
2.0	Purpose	3
3.0	Scope	3
4.0	Background	3
4.1	The Management Of Information Act	3
4.2	IM Program Requirements	4
4.3	The Public Body - IM Mandate	4
4.4	The Role of Public Bodies	5
4.5	The Role of OCIO - Supporting IM	6
4.6	The Role of OCIO - Supporting IT	7
5.0	Recommended Approach	8
5.1	Role of the Public Body – Supporting IM	8
5.2	Assign/Communicate Accountability	8
5.3	Create a Records Inventroy	9
5.4	Define IM Requirements	9
5.5	Create Recordkeeping Guide	13
5.6	Provide Education and Awareness	13
5.6.1	Training	13
5.6.2	Orientation	14
6.0	Definitions and Acronyms	15
6.1	Definitions	15
7.0	Monitoring and Review	17
8.0	References	18
9.0	Appendix A: Records Assessment Template	19
10.0	Appendix B: Information Management Orientation Checklist	21

1.0 Overview

The Management of Information Act (MOIA) requires that each public body must implement an Information Management (IM) program to manage and protect its records. The *MOIA* applies to most public bodies in Newfoundland and Labrador with the exception of Municipalities. The Office of the Chief Information Officer (OCIO) administers the *MOIA* by providing guidance to public bodies to increase overall IM capacity. Many variables, such as size, influence the level of complexity required in an IM program necessary to comply with the *MOIA*.

Public bodies that are large maintain full corporate, administrative and information technology (IT) services. As such, IM program requirements are detailed and resources can be made available to meet them internally. Some examples include: Memorial University of Newfoundland, The College of the North Atlantic, Nalcor, NL Housing, Newfoundland and Labrador Eastern School District and the Regional Health Authorities. For these public bodies the OCIO recommends use of the *Guide to Information Management for Public Bodies* to develop a comprehensive IM program.

Many government public bodies are small and do not have internally supported corporate, administrative and/or IT services. These public bodies take direction on administrative requirements from the departments to which they report. This guideline provides an approach for departments to support these small entities on their IM requirements, which will enable the small entity to fulfill their obligations under *MOIA*.

For the purposes of this guideline, the OCIO uses the public body type indicated below to distinguish between the various references to public bodies that exist with the Government of Newfoundland and Labrador.

Public Body Type	Description
Reporting Entity	Internal public body that is part of core government, i.e.: the Department which an external entity reports.
Large Entity	External public body that <ul style="list-style-type: none"> • is not part of core government • internally supports the corporate, administrative and/or IT services • reports to a government department through its Minister.
Small Entity	External public body that <ul style="list-style-type: none"> • is not part of core government • does not internally support the corporate, administrative and/or IT services • reports to a government department through its Minister • directed on administrative requirements by the departments to which they report.

2.0 Purpose

This guideline provides departments (reporting entities) with external public bodies and those responsible for administering the small entity with an approach to assess and demonstrate compliance with the *MOIA*.

3.0 Scope

This guideline includes elements or issues to consider when assessing IM program needs within a small entity. Features that may determine whether a public body is considered small include but are not limited to:

- May not have the operational need or resources to support independent/internal IM or IT services.
- May not receive centralized Government of Newfoundland and Labrador administrative (e.g. finance, Human Resources) or IT (e.g. government network access, application support) services.
- May be a Category 2 or Category 3 public body under the *Transparency and Accountability Act*.

4.0 Background

4.1 The Management Of Information Act

The Management of Information Act is the primary legislation that prescribes requirements for the management and protection of government records and information. Government records include any media capable of capturing information including paper records, electronic records, email messages, system data, etc. The value of records is dependent on its significance to the event, transaction, activity or process to which it relates and not to its format.

A public body must be able to produce government records to demonstrate how it carried out its mandate. The burden rests with the public body to identify, manage and protect the government records necessary to meet compliance, accountability and transparency requirements. The *MOIA* requires authorization of the Government Records Committee (GRC) to dispose of a government record. This protects public bodies by providing a legal authority to dispose of records. Internal disposal processes are encouraged to ensure there are no known legal issues that require a delay of the disposal (e.g. ongoing litigation, information request made under the *Access to Information and Protection of Privacy Act* (ATIPPA, 2015)). The GRC recommends public bodies have an approved Records Retention and Disposal Schedule (RRDS) to manage its government records. Disposal alternatives include either secure destruction or transfer to the Rooms Provincial Archives for records identified as vital records – permanent retention by the creating public body.

4.2 IM Program Requirements

IM Program requirements vary depending on the size and complexity of a public body as well as the nature of its mandated functions. For example, a transaction-based organization that processes payments in return for licenses, permits or other services varies greatly from that of a policy-based organization engaged in extensive consultation, research and analysis. At a minimum, a public body's IM program should ensure:

- Complete, accurate and reliable records are created to demonstrate the activities undertaken by the public body to meet its mandate.
- Sensitive information, including information that is defined as personal or exempt from public access as per the *ATIPPA, 2015*, is used, shared and stored in an appropriate manner.
- Information and records must be disposed when the public body has met all operational and legal requirements for retention via official methodology. Disposal means either secure destruction under an approved RRDS or transfer to the Rooms Provincial Archives as per the requirements set forth in the *Rooms Act*.

4.3 The Public Body - IM Mandate

Section 2(d) of the *MOIA* establishes those public bodies to whom it applies. It includes all public bodies regardless of their size, budget or complexity and is defined as:

- a department created under the *Executive Council Act* or a branch of the executive government of the province,
- a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown,
- a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a Minister of the Crown,
- a court established under an Act of the province,
- the House of Assembly and committees of the House of Assembly.

A listing of the public bodies to which the *MOIA* applies is located on the OCIO website through the [Legislation page](#).

Section 6 of the *MOIA* provides the following direction to the permanent head of a public body:

Guideline – Managing the Records of External Public Bodies

(1) A permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records.

(2) A system required under subsection (1) shall provide for retention periods and disposition by: destruction, or transfer to the archives, in accordance with the guidelines and schedules established by the Government Records Committee.

(3) A permanent head of a public body shall ensure that the retention, disposal and removal of public records is carried out in accordance with this Act.

4.4 The Role of Public Bodies

Public bodies are directed to meet limited and defined objectives under their overall mandate. Activities may include advisory, adjudicative or regulatory functions as well as provision of services. Public bodies benefit from the ability to engage subject matter experts from the general public. While membership may include public sector employees, public bodies are often composed of individuals that do not have an employment contract with government or access to government resources (e.g. IT). Public bodies provide objective and unbiased services, guidance and decisions.

Public bodies must retain those records required to demonstrate compliance, transparency and accountability. Because public bodies are often accountable to another public body, they must meet common operating and reporting requirements. There are a wide range of public bodies working to support public policy, programs and services across Newfoundland and Labrador. No two share the same mandate, purpose or organization.

However, there are general similarities or characteristics, which include but are not limited to:

- Mandated with a limited or specific set of functions. From an IM perspective this may mean limited types or groups of records (record series) need to be managed.
- Members may be named (e.g. hold a position that is identified by legislation) or appointed through a process prescribed by the *Independent Appointment's Commission Act* and/or the *Public Service Commission Act*.
- May engage a combination of individuals from the general public, industry or trades to participate in activities for which there may or may not be remuneration.
- A member of the public sector may be appointed to a public body as a matter of personal interest outside the scope of their employment role (e.g. a government employee may apply to sit on a regional or special interest committee or council).

Guideline – Managing the Records of External Public Bodies

- A Minister may be appointed to participate in the activities of a public body as a part of his/her portfolio or as a personal interest. The nature of the role in the public bodies' operations may impact how information is managed.
- May operate at arms-length to government and be able to make objective recommendations, decisions, rulings, etc.
- Typically required to report to a central public body such as a government Department or a Crown Corporation.
- May need to comply with government-wide legislation including *The Management of Information Act*, *The Financial Administration Act*, *The Access to Information and Protection of Privacy Act*, *The Transparency and Accountability Act*, etc.
- May receive funding from outside the provincial government and therefore may have additional administrative compliance requirements.

Within this larger group, those defined as small:

- May have a small or limited operating budget to support mandated functions. This number typically falls under \$50,000 annually. Some public bodies rely on a central public body to administer operating funds (e.g. marketing campaigns) or to reimburse individuals for travel or expenses associated with their role in the public body (e.g., hotel, taxi, airfare). Such records are necessary to support compliance with the *Financial Administration Act (FAA)*.
- Have fewer than 15 individuals engaged in work on the public body's behalf.
- Have limited or no access to administrative or IT resources. Large public bodies have an internal administrative complement or are likely provided direct access to the public bodies' support infrastructure.

The limited size and scope of a smaller public body does not reduce the accountability under the *MOIA* to manage and protect information.

4.5 The Role of OCIO - Supporting IM

The OCIO administers the *MOIA* and provides centralized IM services to government departments and some public bodies. In this role, the OCIO will assist the department in providing IM support to public bodies.

To support this mandate the OCIO manages the following activities, programs and services:

- Develops IM policies, directives, standards and guidelines for government as authorized by TBM2009-335 *Information Management and Protection Policy*.
- Provides direction on IM best practices, resource requirements, organizational structure and IM systems for government.

- Assists departments/agencies to improve their IM capacity.
- Provides IM consultancy services and support to public bodies.
- Supports the IM Community, consisting of IM representatives from government departments and supported public bodies.
- Manages the Provincial Records Centre (PRC).
- Supports the Government Records Committee (GRC).

Note: The OCIO Directive, Use of Non-Government Email for Work Purposes, clearly establishes that the use of non-government email is not permitted for government business. There is an exception process, but this must be managed by the head of the public body (e.g. Deputy Minister, CEO, etc.). It is recommended that public bodies discuss this process with the department responsible for their administration/support to ensure email processes used are in keeping with this directive.

4.6 The Role of OCIO - Supporting IT

Over 150 entities fall under the *MOIA*, but only half receive IT support from OCIO. For these entities, the OCIO has authority to provide all IT/IM services. Decisions around the level of support required are based on resource availability, collaboration requirements and the sensitivity of the information maintained. Direct IT support may be required for a tribunal, appeals board or commission managing individual cases or claims containing sensitive information. In such instances, the public body's Planning Service and Delivery Committee (PSDC) will engage the OCIO through Client Services Division to determine requirements. IT support must be approved by a permanent head or designate and may include the following, as well as, other services:

- Development/maintenance of a website,
- Development/maintenance of content/collaboration websites,
- Provision of government-issued email accounts to individuals,
- Remote Access tokens,
- Access to the government network or IT assets (e.g. Network File share, Business Application),
- Provision of equipment (e.g. Laptops, Tablets, Encrypted Portable Storage devices, etc.),
- Access to Government email accounts.

5.0 Recommended Approach

This guideline provides departments (and small entities which report to those departments), with an approach to assess and implement IM program components necessary to meet and show compliance with the *MOIA*.

Activities recommended may include but are not limited to:

1. Complete an Initial Planning Session
2. Assign/Communicate Accountability
3. Create a Records and Information Inventory
4. Define IM Requirements
5. Modify/Finalize Business Rules Document
6. Provide Education and Awareness

5.1 Role of the Public Body – Supporting IM

A reporting entity (e.g. department) may provide a small entity who reports to the same Minister with guidance on compliance requirements. This role may be assigned to a director-level resource in the reporting entity, normally Information Management or Policy and Planning, Corporate Operations.

Decisions made regarding the engagement of the small entity in the reporting entity's IM program will need to be assessed on a case-by-case basis. Different decisions may be made to manage the records of a tribunal that deals with sensitive personal or health information than that of a council or committee that maintains publicly accessible information (e.g. is contained in the annual report, published minutes or would be released under *ATIPPA, 2015*).

An initial planning session is recommended in order to make these determinations.

5.2 Assign/Communicate Accountability

Under the *MOIA*, Section 6, the permanent head of a public body (reporting, large and small entities) is mandated to implement a program to manage and protect government records and information. This will typically be a Deputy Minister, Chief Executive Officer, Chief Operating Officer, President or Chief Information Officer. Small entities may feature a variety of roles with this level of accountability. It may, for example, fall to a Chairperson who is appointed by a Minister to hold this position.

The reporting entity should issue a communication to the permanent head to:

- Outline the *MOIA*

Guideline – Managing the Records of External Public Bodies

- Invite the small entity representative to the IM Community of practice maintained by the OCIO
- Identify IM services available to the small entity by the reporting entity, the OCIO, etc.
- Request/communicate assignment of a lead from the small entity
- Request completion of a records inventory for the small entity
- Communicate plans to define IM requirements

The OCIO IM Advisory Services are available to assist in developing templates for this communication.

5.3 Create a Records Inventory

One of the first tasks for the small entity will be to identify and list all of the current information holdings within their storage locations. The OCIO Guideline, *Records and Information Inventory*, provides useful information for how to complete this task. This inventory will provide a critical input to the requirements process. The OCIO also provides training on how to complete an inventory.

5.4 Define IM Requirements

Critical to a good IM program is getting the right information, to the right person at the right time. Components or issues for consideration when identifying requirements may include but are not limited to:

Background

- **Mandate:** Overview of the small entity's mandate as outlined in annual reports or other documentation provided by the lead.
- **Operating Requirements:** Does the small entity operate on a full-time or part-time basis. Numerous small entities are established to operate on a part-time basis (e.g., council, committee or tribunal).
- **Individual Engagement:** Small entities benefit from the ability to engage the public in participation. This often means that individuals engaged to perform work on behalf of the small entity may or may not have an employment contract with a public body. It would be helpful in determining requirements to have:
 - A general idea of the type of engagement the individuals typically have – employee, volunteer, term-based, etc.

Guideline – Managing the Records of External Public Bodies

- A public sector employee that participates as a part of their assigned work duties? If so then this individual has access to the government network and/or IT resources. Is it appropriate for this individual to be assigned accountability for retention and storage of records?
- **Funding Sources:** Small entities may be funded outside the provincial government. For example, the federal government may provide funding and may impose record creation and/or reporting requirements.

IM Assessment and Advice

- **Review and Approval Process:** Identify who will be engaged to approve IM program deliverables such as the RRDS, and identify who is responsible for implementing deliverables. Ensure this resource and others supporting IM have the necessary support and training to start the IM program for the small entity.
- **Location of Work:** The small entity may or may not have a dedicated work location. It may rely on the use of public buildings or alternatively it may procure locations from private sector (e.g., conference centre, hotel meeting space) to hold meetings or collaborate on deliverables. From an IM perspective, this may mean that there is no onsite storage location for records. The small entity will need clear guidance on the use of public space to complete work, use of portable storage, safe meetings, how and where to safely store records, and overall treatment of records in storage.
- **Confidentiality Agreements:** When an individual is engaged in the work of the small entity, are they required to sign a confidentiality agreement? If so, does this agreement reference records and information? Does it need to be modified to accommodate the IM program requirements? The IM representative should ensure such documents are properly completed and stored.
- **Record of Authority:** Who will be responsible for retention and storage of records and information? The small entity will need to advise each member what his or her requirements are in relation to IM. The objective of the IM program is to ensure the retention of a complete, accurate and reliable record of authority. Depending on the type of engagement individuals have with the small entity, there may be copies of information held by those individuals externally. Guidance needs to be clear on where the records are and what individuals should do with copies. Copies of sensitive information, for example, may not be permitted and/or individuals may be advised that such records should be returned to the small entity for secure destruction.
- **Record Series:** What records series are generated by the small entity? Follow up with knowledgeable individuals on the content of the inventory to identify the record series maintained by the small entity. Some complex record series may require the identification of records series secondary and tertiary subseries.

Guideline – Managing the Records of External Public Bodies

- **Records Creation:** Based on the record series and subseries, it is important to identify what records are created to support the processes of the small entity. An assessment template is included in Appendix A to assist. Use the results to identify which records need to be retained to support compliance, accountability and transparency requirements. Where appropriate, create forms and templates to be used by the small entity. IM Advisories are available on the OCIO Website provide links to guide individuals on appropriate records creation for:
 - Executive Records
 - Program Administration
 - Case Files
 - Meeting Records
 - Note To File
- **Record Labelling and Organization:** Based on the record series provide instruction on how the records should be labelled and organized.
- **Publication Process:** Under the *Rooms Act*, the Legislative Library is the official repository for all published materials. Public bodies, reporting, large and small entities, are advised to transfer up to three copies of published materials to the legislative librarian for permanent retention. Based on the assessment of the record series and creation requirements it is possible that all records that need to be retained are published and therefore transferred to the legislative library. This would mean that the small entity may need only ensure appropriate secure destruction of transitory records
- **RRDS and/or One Time Disposal (OTD):** When ready, the small entity should schedule their records for retention/disposal. Based on the record series, complete the RRDS Template for Operational Records available on the OCIO website. OCIO's IM Advisory Services can be engaged to support the process and it is recommended that consultation occur early on in the process. The inventory may have revealed a backlog of records that require immediate disposal. Follow the one time disposal process outlined on the OCIO website.
- **OTD:** One time disposal inventory may have revealed a backlog of other records that require immediate disposal that will not be part of a RRDS. Follow the one time disposal process outlined on the OCIO website.
- **Collaboration:** Based on the process analysis, how do the members of the small entity collaborate and communicate? It is likely that individuals rely heavily on email to transfer content and then may save information locally for review/editing. Based on the level of sensitivity (e.g., personal information, health records, etc.) the small entity may decide it needs to develop secure transfer/collaboration processes.

Guideline – Managing the Records of External Public Bodies

- **Email Usage:** Government-issued email accounts should be the standard method used for conducting public body business. However, depending on the engagement of the individual, government-issued email may not be used. Individuals may feel they can rely on the use of personal email accounts to complete small entity work - exposing government records to potential lack of access or loss/destruction while in private sector storage. As noted earlier, the OCIO has a clear directive not allowing the use of non-government emails for government work unless there is a well-documented exception process as approved by the head of the public body. The department to which the public body reports, the reporting entity, will need to assess the appropriateness of using personal information on a case-by-case basis and establish an exception for the small entity if required. Please review the [Non-Government Email Directive](#).
- **Storage:** Storage of electronic and physical records is assessed on a case-by-case basis. Clear guidance should be provided to ensure the safety and security of government records. The OCIO has a number of documents to assist in [Information Management and Protection](#).
 - Storage considerations may include:
 - Use of public facilities for storage of physical records
 - Third party storage for physical records
 - Individual storage of physical record
 - Storage of government records on the public body's network (e.g., PSNL for public bodies that receive IT services from OCIO)
 - Storage of records on private individual home or business network – clear documented, provisions to transition this information to government records needs to be established
 - Where appropriately established based on the types of records, and clear direction is provided to the small entity, use of [cloud-based storage](#)
 - Use of encrypted portable storage devices
- **Secure Destruction:** The *MOIA* requires secure destruction of records including those in electronic media. Secure destruction can be completed onsite or through a vendor as outlined in the OCIO Guideline [Disposal of Records](#).
- **Termination:** Small entities may have individuals engaged for a set time period after which the responsibilities may be transferred to others (e.g., a new council is appointed). Individuals need clear direction on what happens to any records, tools, equipment, etc. in their possession at the end of the

term. Access to any government resources, assets or applications must also be terminated at this time; the reporting department should ensure appropriate procedures are in place in the department, reporting entity, and the small entities for these transitions.

- **Services Provided by the Public Body:** The reporting entity will need to determine on a case-by-case basis what IM-related services will be provided to a small entity. Many variables may impact the decision making including the requirements defined for compliance, existing engagement of internal employees, provision of other administrative service (e.g., finance, HR), resource allocation and level of sensitivity of information maintained. The services to be provided should be articulated in the business rules or reference document and be approved by any applicable central agency (e.g. HRS, Finance) if required.

5.5 Create Recordkeeping Guide

Based on the requirements identified in Section 5.4, the small entity should create a Recordkeeping Guide document that includes the IM requirements in a central authoritative reference document. This document should be provided to all individuals engaged in work on behalf of the small entity. This provides a central reference document for all members/employees. A separate guideline **Recordkeeping Guide** is available that can be modified to accommodate the small entities requirements.

5.6 Provide Education and Awareness

5.6.1 Training

The OCIO has extensive training and support resources available on its Website. This includes:

- **IM@Work: Making Information Management Work for You** - This presentation provides general guidance on the *MOIA*, individual responsibilities and best practices to manage and protect information. It is suitable for all individuals engaged in work on behalf of a public body..
- Quick Reference materials available on multiple topics which include: Safe Business Practices, Password Management Best Practices, Recommended Approach to Encrypting GNL Files, Safe Email Practices, etc.
- OCIO IM Advisories are available on a range of subjects including Meeting Records, Case Files, How to Prepare Records for Transfer.

5.6.2 Orientation

Provide new members/employees with an overview of the recordkeeping guide. A checklist has been included in Appendix B that summarizes the recordkeeping requirements.

6.0 Definitions and Acronyms

6.1 Definitions

Archival Records – are records that are preserved because of their continuing value. The Rooms Provincial Archives is the organization mandated to collect, preserve, present, exhibit and make available for research the archival records that represent and illustrate the significant history, culture and natural heritage of the province of Newfoundland and Labrador (source: *Rooms Act SNL2005 CHAPTER R-15.1*).

Government Records Committee (GRC) - The GRC is the official body that is mandated to review and revise schedules for the retention, disposal, destruction or transfer of government records, make recommendations to the minister respecting public records to be forwarded to The Rooms, Provincial Archives, authorize disposal and destruction standards and guidelines for the lawful disposal and destruction of public records and make recommendations to the minister regarding the removal, disposal and destruction of records (source: *Management of Information Act SNL2005 c.M-1.01*).

Government Record - means a record created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and an abandoned record.

Information Management (IM) - is a program of records and management of information practices instituted to provide an economical and efficient system for the creation, maintenance, retrieval and disposal of government records. Under the Management of Information Act SNL2005 c.M-1.01, the permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records.

Information Technology (IT) – means technology involving the development, maintenance, and use of computers and software for the processing and distribution of information.

Office of Primary Responsibility (OPR) - is the organization and/or position and/or division within an organization that is responsible for maintaining the integrity of a record (source: Corporate Records and Information Management Standard (C-RIMS)).

Public Body - "public body" means a department created under the Executive Council Act or a branch of the executive government of the province, a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown, a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a minister of the Crown, a court established under an Act of the province, and the House of Assembly and committees of the House of Assembly;

Record – A record means a correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic (Source: Management of Information Act SNL2005 c.M-1.01).

Records Retention and Disposal Schedule (RRDS) - A records retention and disposal schedule is a legal document that guides the management of a government record. A RRDS will define the content of the record series or types, link the records to the organizational unit and business process, dictate how long the records need to be retained in active and semi-active storage to meet operational and legislative requirements, and authorize the disposal of information in a legal manner including either secure destruction or transfer to the Rooms Provincial Archives. It can also identify vital records that need to be permanently retained by a department or agency.

Transitory Record - A transitory record is a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can be securely destroyed when no longer of value without authorization of the Government Records Committee (source: Management of Information Act SNL2005 c.M-1.01).

Vital Record - A vital record is defined as one that is indispensable to a mission critical business operation or a record identified as essential for the continuation of an organization during or following a disaster. Such records are required to recreate the organizations legal and financial status and to support the rights and obligations of employees, customers, shareholders and citizens (source: Making the Transition from Paper to Electronic, David O. Stephens, ARMA International, 2007).

Acronyms

ABC	Agencies, Board and Commissions
ATIPPA	<i>Access to Information and Protection of Privacy Act, 2015</i>
CRIMS	Corporate Records Information Management Standard
GRC	Government Records Committee
IM	Information Management
IT	Information Technology
MOIA	<i>Management of Information Act</i>
RRDS	Records Retention and Disposal Schedule

7.0 Monitoring and Review

The Information Management Services Division of the OCIO is responsible for monitoring and reviewing this Guideline in accordance with processes set forth by the Application and Information Management Services Branch.

8.0 References

Include Links to all published information referenced in the document including:

Management of Information Act

Rooms Act

Transparency and Accountability Act

Access to Information and Protection of Privacy Act, 2015

Information Management and Protection Policy, TBM 2009-335

OCIO Guideline

Managing Departmental Information Through the Employment Cycle

OCIO Standard

One Time Disposal

OCIO Directive

Acceptable Use of the Government Network and Information Technology Assets

OCIO Guideline

Records Disposal

OCIO Quick Reference

Safe Business Practices

OCIO Quick Reference

Safe Email Practices

OCIO Quick Reference

Password Management Best Practices

OCIO FYI Encrypting Files

Encrypting Files with 7-Zip and WinZip

9.0 Appendix A: Records Assessment Template

The *Management of Information Act* requires public bodies to create such records as are reasonably necessary to document business decisions. This records assessment form has been developed to enable an employee to assess business activities their practice area is responsible for the purpose of identifying associated records.

Step One: Make a list of all the business processes that your organization is responsible for

Step Two: For each of the processes, complete the table below. Additional tables can be added by simply copying and pasting the table below.

Records and Information Assessment	
Identify the business process that resulted in the creation of these records.	
Who initiates the process? Is there a document or piece of information created to initiate the process?	
What are the steps that occur to complete the process? Are more documents or records created as a result of the process? What are they?	
What information is required to complete the process? Complete the transaction? Provide the service?	
Are records scanned into the TRIM Content Management System? Who performs this function? What happens to the original paper?	
Who is involved in this process? Internal staff? Other Government Departments? External Stakeholders?	
Who is responsible/accountable for the execution of this process?	
How often does the activity/process occur? Daily/Weekly/Monthly?	
What is the anticipated volume?	

Records and Information Assessment	
Is the process regularly scheduled?	
Is the process related to a larger program? Identify is applicable.	
What is the outcome of the process? How is this documented?	
Once the process is complete, how often do you need to access the records? Is it more than once every 3 months? 6 months? Maybe Never?	
Are the records physical, electronic or both? Where are copies of records retained?	
How are the records organized? Is the same organization applied to all formats?	
Who is responsible for keeping records organized?	
Is the organization of the records documented anywhere?	
Are there any specialized media (e.g., video, audio, photos, negatives)	
Is there an IT system related to these records? Identify it and provide a contact name.	

10.0 Appendix B: Information Management Orientation Checklist

New Employee/Individual Record Keeping Checklist Template

Using a checklist when providing orientation to a new employee or individual engaged to perform work on behalf of the small entity may be helpful in ensuring all elements are communicated and understood. Checklist items are based on the content of the small entities' Record Keeping Guide. As such, each checklist will reflect the small entities' unique requirements. The following list includes common elements that may be discussed when a new individual is engaged to perform work on behalf of the small entity. Elements may be deleted/added as required.

- IM@Work - Reviewing the document on the OCIO website will provide a general overview of Information Management (IM), The *Management of Information Act (MOIA)*, individual responsibilities, and best practices.
- Identify known records to be created/maintained by the individual
- Identify duration/retention of information
- Identify forms/templates to be used and where they are located
- Review compliance requirements for collection/management of personal information (if relevant)
- Review email usage requirements
- Review how/where records are organized/stored
- Allocate IT resources/equipment:
 - Laptop/personal computer
 - Tablet
 - Portable storage device
- Review disposal requirements and secure methods for destruction

Please note there may be other additional orientation required (e.g. financial, privacy etc.)



7. F.Y.I

- 7.1. Acceptable Use of the GNL Network and/or Assets
- 7.2. Which Records to Store in HPRM
- 7.3. Secure Storage and Disposal of Physical Records
- 7.4. Instant Messaging Directive
- 7.5. Identifying and Disposing of Transitory Records
- 7.6. Identification and Disposal of Government Records
- 7.7. Records Retention and Disposal Schedule
- 7.8. IM Advisory – Case Files
- 7.9. IM Advisory – Executive Records
- 7.10. IM Advisory – Meetings Records
- 7.11. IM Advisory – Note to File
- 7.12. IM Advisory – Program Administration Records
- 7.13. IM Advisory – Preparing Paper records for Offsite Storage
- 7.14. IM Advisory – Retrieving Records from the PRC
- 7.15. IM Advisory – Transferring Records PRC

Overview

CIMFP Exhibit P-04489

Page 308

In support of its mandate, the Office of the Chief Information Officer (OCIO) is responsible for the protection, security and management of the 'Government Network' and government information technology (IT) assets. It is critical that the Network and government IT assets are protected from unauthorized or inappropriate access or use. Inappropriate access or use of the Network and/or government IT assets, either knowingly or unknowingly, exposes the Employer to risks that may compromise the protection, security and performance of its information, IT systems and services.

To reduce the risk of inappropriate access or use of the Network and/or government IT assets, the OCIO has released the *Acceptable Use of the Government Network and/or IT Assets Directive*.

Key Points

- ▶ The OCIO can issue directives, standards and guidelines across Government under the authority of the *Information Management and Protection Policy* (TBM 2018-111 which replaces TBM 2009-335). For more information, see https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.html.
- ▶ The purpose of this Directive is to reduce the risk of inappropriate access or use of the Network and/or government IT assets by informing and educating end users of:
 - ▶ Appropriate and acceptable end user behavior when using the Network and/or government IT assets, including the end user's role in protecting and securing the Network and these assets; and
 - ▶ OCIO's authority to undertake specific actions where required to securely manage and protect the Network and its IT assets, including the right to monitor the Network and its activity, as well as access government IT assets.
- ▶ This Directive was developed after extensive consultation with the Department of Justice and the Human Resource Secretariat (HRS); it aligns with HRS's *Equipment Resource Usage Policy* (see http://www.exec.gov.nl.ca/exec/hrs/working_with_us/equipment_and_resources.html) and addresses potential privacy concerns related to the monitoring of network activity.
- ▶ This Directive applies to all Government departments and public bodies supported by the OCIO; it is mandatory to follow. Employees, in this context, applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons entrusted to access or use the Network and/or government IT assets.
- ▶ This Directive applies to IT assets owned by Government or devices approved for use on the Network.
- ▶ The OCIO will continue to promote education and awareness of 'Acceptable Use' by incorporating its key messages into existing training and education channels.

Which Records to Store in HPRM (TRIM)

Definition

HPRM(TRIM) is the Government of Newfoundland and Labrador's standard Electronic Document Management System (EDMS). An EDMS is used to manage everything that happens to a record including creation, sharing, collaboration, storage and destruction. Records managed and stored in HPRM are either created using desktop software (e.g., Microsoft Outlook, Word) or are paper records that are digitized using a scanner.

Issue

The type of records included in HPRM impacts on its implementation, use and maintenance. For example, if the workflow feature is used to automate a business process, then effort is required to program the process in HPRM and to train employees to replace the existing manual process. This is why analysis of the types of records that will be stored in HPRM is required in the planning stage.

Advice

Factors to consider when deciding which records to store in HPRM include:

- Purpose of the Record Series: Records that support departmental programs and services may be of a higher priority to users than others (e.g. administrative, reference).
- Office of Primary Responsibility (OPR):
 - Placing records into HPRM for which the department is the OPR ensures that operational and legal requirements for retention and disposal are met.
 - If the department is not the OPR, it has no legal obligation to manage the record. It is the department's responsibility to ensure that the OPR's disposal requirements are adhered to.
- Volume of Use: Records accessed at a higher rate benefit from centralized storage in HPRM where there are multiple ways to access them quickly.
- Type of Use: Understand how using HPRM will support the business processes associated with the records. For example, it may be more beneficial to focus on records that support transactional processes such as client requests than records that will be used solely for reference.
- Length of Retention: Records with a longer retention requirement will benefit from HPRM where proper classification and application of retention requirements are applied at the time of capture.
- Retention Format: Consider whether there any requirements that preclude the retention of this information in electronic format (e.g., legislative requirements for records to be retained in signed-off paper format). Departments that wish to digitize records in HPRM must get approval from the Government Records Committee to dispose of paper originals.

More Information

Information regarding HPRM is available by contacting IM@gov.nl.ca



Secure Storage and Disposal of Physical Records

Definition

Physical records are tangible objects that contain recorded information. Examples include paper, parchment, manuscripts, maps, plan, drawings, paintings, prints, photographs, magnetic tapes, computer discs, microform and other documentary material. The term records disposal includes either physical destruction or deletion or the transfer of records to a third party such as the Rooms Provincial Archives or another public body.

Issue

- ▶ The loss, damage or inappropriate disclosure of physical records may have serious implications.
- ▶ Incorporating best practices for secure storage and disposal of physical records into your daily routine minimizes risk.

Advice

- ▶ Members of the public, meeting attendees, maintenance staff, contractors and vendors often need to access your work area:
 - A "clean desk" practice can limit unauthorized access to information
 - File cabinets in hallways and common areas must be locked at all times
 - Records boxed for transfer must be stored in a locked room
 - Records must not be left unattended in public areas.
- ▶ If the records are authorized for destruction then they must be securely disposed of in a manner that makes the content unreadable including:
 - Shredding records in on-site office shredders
 - Placing records in secure shredding bins.
- ▶ When preparing records for storage:
 - Complete documentation to support tracking and retrieval
 - Supervise physical transfer and obtain appropriate sign-off of receipt/transfer.
- ▶ Designated records storage rooms including information services centres, storage rooms, records centres or vaults must have:
 - Employee(s) assigned to manage use
 - Appropriate security procedures in place to control and monitor access
 - Documented procedures for removing and returning information, etc.
 - An up-to-date inventory of holdings
 - Periodic audits for potential risks (e.g. flooding, infestation, etc.).
- ▶ Use alternative storage locations to accommodate records that cannot be safely stored onsite:
 - Third party offsite storage: Provides secure storage for all information. Contact your financial operations officer for access to the Master Standing Agreement for File Storage
 - Provincial Records Centre: Provides secure storage for government records that fall within its mandate.

More Information

- ▶ Discuss with your manager or your department's information management staff.
- ▶ General inquiries can be directed via Email to IM@gov.nl.ca.



A purple circular icon containing a white speech bubble with the letters 'FYI' inside. The icon is positioned in the top right corner of the page, overlapping a decorative graphic of colorful curved lines.

Instant Messaging Directive

Overview

Instant messaging technologies are designed to support real-time conversational interactions and are commonly used to facilitate the flow of business. These technologies are not an appropriate medium for record-keeping due to challenges with managing and searching for data. Instant messages are discoverable for legal, audit or access to information requests and must be managed appropriately.

Definition: Instant messaging is a form of real-time, direct communication between two or more parties using personal computers or other devices such as smart phones or tablets. Instant messaging technologies are designed to support real-time conversational interactions. Examples of instant messaging include: Blackberry Messenger (BBM), Text Messaging (includes messages sent via Short Message Service (SMS), Multimedia Messaging Service (MMS) or iMessage) and Skype for Business.

Advice

- For the most part, instant messages tend to be transitory records with short-term value and do not need to be stored and managed in a records management system. Transitory records are of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.
- Occasionally, an instant message conversation will evolve into a discussion that has business value and must be managed as a government record.
- If an instant message is determined to be a government record it must be managed appropriately by transferring it to an approved government recordkeeping format. It is the content of a message, not its format, which determines whether it is a government record.
- Once the conversation evolves into information that should be retained as a record, the quickest way to transfer the content to an appropriate medium is to send an email to all those involved in the conversation.

(See QUICK REFERENCE – Transitioning Instant Message Content to Recordkeeping Format)

- Instant messages retained on a mobile device should be regularly reviewed by the owner of the device. It is not necessary to retain instant messages that have been determined to be transitory. These transitory records can be disposed of without approval from the Government Records Committee (GRC).

Descriptions of the above noted instant messaging technologies are listed on the following page.

Instant Messaging Technology Descriptions

Blackberry Messenger (BBM)

Blackberry Messenger is a proprietary Instant Messaging application now available for use on most smart phones.

Text Messaging (SMS, MMS and iMessage)

Text messaging is the text communication service component of phone, web or mobile communication systems, using standardized communications protocols that allow the exchange of messages between fixed line, mobile phones, tablets and other devices. Text messaging can have many formats including Short Message Service (SMS), Multimedia Messaging Service (MMS) or iMessage.

Skype for Business

Skype for Business is a type of SMS messaging. It is a real-time communications system providing enterprise instant messaging, peer to peer and multiparty voice and video calling. These features can be available within an organization, between organizations, and with external users on the public Internet.

For more information on the Instant Messaging Directive contact IM@gov.nl.ca.

Supporting Materials

Version History

(OCIO Ref. DOC02854/2018)

POLICY—Information Management and Protection Policy

https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.pdf

Version 1 2012 02 01

Version 2 2018 09 24

DIRECTIVE—Instant Messaging Directive

https://www.ocio.gov.nl.ca/ocio/instant_messaging_directive.pdf

FAQ—Instant Messaging Directive

https://www.ocio.gov.nl.ca/ocio/instant_messaging_faq.pdf

FYI—Identifying and Disposing of Transitory Records

<https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/transitoryrecords.pdf>

GUIDELINE—Email Guideline

<https://www.ocio.gov.nl.ca/ocio/publications/policies/emailGuidelines.pdf>

QUICK REFERENCE—Transitioning Instant Message Content to Recordkeeping Format

https://www.ocio.gov.nl.ca/ocio/instant_messaging_quickreference.pdf



FYI

Identifying and Disposing of Transitory Records

Definition

Transitory records are defined in the Management of Information Act as government records of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

Advice

- Transitory records are either copies of information retained elsewhere or records that will not be required as evidence of government's business activities.
- Transitory records may be disposed of when they are no longer of value, and shall only be disposed of through means which render them unreadable, including secure shredding or, in the case of electronic records, secure electronic erasure.
- Disposing of transitory records in a timely manner facilitates efficient use of resources as storage and management requirements for these records is minimized.
- Disposing of transitory records does not require authorization of the Government Records Committee.
- If in doubt whether to keep or dispose of transitory records, discuss with a manager or your department or other public body's information management staff.

Examples

Convenience copies of information retained for reference purposes:

- Copy of a report of a government record available in an alternate location and format
- Extra copies of meeting agendas and minutes
- Electronic version of a signed document, where it has been determined that the signed version is the record to be kept and managed

Drafts of records:

- Which reflect content that is included in the final version of the record
- Which contain only minor edits to content or formatting changes

Supporting information used in the preparation of a subsequent record:

- Working papers, notes and research deemed to be inconsequential

Records not directly related to you or your office that do not require you to act:

- E-mails on which you are in the “cc” line only – once you determine you no longer need to retain “cc’s” you may delete them

Transmittal or routing slips and opened envelopes:

- A physical routing slip or an e-mail that is used to route an attached document – “see attached” e-mails
- E-mail read receipts or failure receipts

Broadcast messages sent to all employees:

- Invitation sent to all employees, PSN e-mail messages
- Notice of renovations and employment opportunities

Publications produced for mass distribution:

- Catalogues, periodicals, pamphlets and newsletters

For more information on Transitory Records contact IM@gov.nl.ca.

Supporting Materials

POLICY—Information Management and Protection Policy

https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.pdf

DIRECTIVE—Instant Messaging Directive

https://www.ocio.gov.nl.ca/ocio/instant_messaging_directive.pdf

FAQ—Instant Messaging Directive

https://www.ocio.gov.nl.ca/ocio/instant_messaging_faq.pdf

FYI—Instant Messaging Directive

https://www.ocio.gov.nl.ca/ocio/instant_messaging_fyi.pdf

GUIDELINE—Email Guideline

<https://www.ocio.gov.nl.ca/ocio/publications/policies/emailGuidelines.pdf>

QUICK REFERENCE—Transitioning Instant Message Content to Recordkeeping Format

https://www.ocio.gov.nl.ca/ocio/instant_messaging_quickreference.pdf

Version History

(OCIO Ref. DOC02856/2018)

Version 1 2012 02 01

Version 2 2018 09 24



Definition

Government records are defined in the *Management of Information Act* as records created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and abandoned record.

Advice

- Government records:
 - ▶ Control, support or document the delivery of programs or services
 - ▶ Support the decision making process
 - ▶ Document activities of the department
- The *Management of Information Act* requires that the disposal of government records must be authorized by the Government Records Committee. A records retention and disposal schedule is the preferred authorization tool.
- A disposal authority is required to ensure that any specialized legal requirements for retention and disposal are met including:
 - ▶ Extended retention in semi-active storage to meet legal requirements
 - ▶ Transfer to archives
 - ▶ Secure destruction
- If in doubt as to whether a record is a government record or not, discuss with your manager or your department's information management staff.

Examples

Records that document a transaction:

- ▶ Processing of an application for a license, receipts or claim processing documents

Records that document the provision of a government service:

- ▶ Case files, client files, work orders or service reports

Records that reflect program or project development and/or implementation:

- ▶ Meeting minutes or project management records

Original versions of publications that are filed by the program area responsible:

- ▶ Annual Report, Business Plan,

Significant drafts that demonstrate stages of development or decision making:

- ▶ Updates to cabinet records, policy documents, legislation or project records

Records of recommendations and decisions including relevant supporting material:

- ▶ Executive or senior-level briefing notes, Cabinet advice, memos to senior management and executive or reports from consultants

Records that document service to the public:

- ▶ Completed application forms, notice of assessment, or request for additional information to complete a claim

Records that document deliverables to be provided by consultants, vendors or contractors:

- ▶ Contracts, statements of work or receipt of deliverables
- ▶ Communications that clarify requirements or establish timelines

Records of Policy and Planning activities:

- ▶ Final version of the annual business plan, departmental operational plans or work plans



Definition

A Records Retention and Disposal Schedule (RRDS) prescribes requirements for the length of time a government record must be retained and the appropriate means of disposal at the end of its lifecycle. Retention and disposal requirements may be driven by legislation, regulation, policy, legal precedent, best practice, or agreement with a third party (such as another level of government).

Advice

- ▶ Under the *Management of Information Act*, a government record "...shall not be destroyed or removed from the ownership or control of the Crown unless the destruction or removal is authorized under this Act."
- ▶ Departments and other public bodies, as defined in the Act, should develop an RRDS for groups of records under their authority, so that they may legally dispose of those records. In order to legally implement a RRDS, it must be authorized by the Government Records Committee (GRC).
- ▶ The Corporate Records and Information Management Standard (C-RIMS) has been developed by the Office of the Chief Information Officer (OCIO) as a standard RRDS for records which are common across all departments and public bodies: including human resources, general administration, facilities management, financial management, information and information technology management, and equipment and supplies (material) management. These records are called corporate (or sometimes administrative) records.
- ▶ Operational records are those that reflect the unique mandate of their creators. Records of programs, projects, and service delivery are examples of operational records. Unlike corporate records, these will be different in each organization. Each department or public body is responsible for the development, implementation and maintenance of an RRDS for operational records under their authority.
- ▶ If in doubt as to whether a record is a corporate record, and therefore can be addressed using C-RIMS, or an operational record and therefore requires its own operational RRDS, consult with your department's Information Management staff, or the description of C-RIMS on the OCIO website [Corporate Records and Information Management Standard (C-RIMS)].

An RRDS for Operational Records Should Contain Information About:

- ▶ The organization that collected created or received the records
- ▶ The content of the records including the type of information contained within them
- ▶ The purpose of the records, including the business process associated with their collection, creation and use
- ▶ The creator custodian of the records
- ▶ The format of the records (e.g., paper, electronic, photograph, etc.)
- ▶ Records which contain personal information and therefore require protection
- ▶ Records which contain information which may cause a mandatory exemption under the *Access To Information and Privacy Protection Act*
- ▶ Information on how records are organized
- ▶ Storage locations (both on-site and off-site)
- ▶ Storage requirements (how long records need to remain onsite to support ongoing operations, how long records need to be retained in semi-active storage to comply with legal requirements for retention on the part of the department)
- ▶ Means for disposing of records (secure destruction using best practices outlined on the OCIO website, or transfer of records determined to have enduring value to The Rooms Provincial Archives)
- ▶ Organizational contacts (individuals within the organization who must be engaged in implementing and monitoring the RRDS, such as Information Management staff and the department's or public body's ATIPP Coordinator)


FYI

IM Advisory — Case Files

Overview

This Office of the Chief Information Officer (OCIO) Information Management (IM) Advisory provides common best practices to consider when managing case files. The audience for this advisory includes all public bodies as defined under the Management of Information Act. Public bodies may develop additional requirements to meet individual needs. Public bodies are advised to consult with their internal IM division to access internal requirements, tools and services. This advisory supplements resources available on the OCIO website.

What are Case Files?

A “case” is any project, transaction, service or response that is “opened” and “closed” over a period of time to achieve resolution of a problem, claim, request, proposal, development or other complex activity. It is likely to involve multiple persons inside and outside of the organization, with varying relationships to each other, as well as multiple documents and messages (Source Aiim.org).

While the term “case file” may not be used, many processes or services have an identifiable start/end date and result in the assembly of similar or repetitive groupings of records. The most effective means of managing the records produced is as a unit or case file. Examples of processes/services include but are not limited to:

- Client Management
- Employee Management
- Certificates Processing
- License Processing
- Service Requests
- Claims Processing
- Project Management
- Inspections
- Issues Payments
- Incident Management
- Complete Assessments
- Issue Permits

Why Manage Case Files?

Case files often represent a core function or service of the public body. They are often linked to an individual, client, vendor or third party that has dealings with government or a project program or initiative. Applying effective case file management is beneficial as it may ensure:

- The operational requirements to support daily work are met and documented.
- Only the information the public body is authorized to collect is retained.
- Appropriate access control can be established if personal or confidential information is captured.
- Information is accessible in the event of a reference or legal request (e.g. request under the Access to Information and Protection of Privacy Act, 2015).
- Compliance with legal requirements for retention and disposal.

Things to Consider When Managing Case Files

Employees should have clear direction on how to manage the information used to administer or carry out programs and activities on behalf of the public body. This information may be documented in a training or support manual. Programs or services may have requirements that are unique to the type of information or service as determined by the public body. General considerations when creating information management policies and procedures may include, but are not limited to:

Define Who Should Document: Establish clear requirements for documenting case files up front with your manager or supervisor, including who is responsible for documentation.

Define the Business Process: Case files are typically related to the provision of a program or service to an individual or third party (e.g. vendor). Processes associated with these programs or services should be well defined and consistently applied. The records generated through the process form the complete case file or record. Suggested activities for consideration include:

- Document the steps typically required to complete the process (e.g. open file, enter data, apply payment, print certificate, make file copy, draft and sign correspondence, return to applicant, close file).
- Multiple employees may need to access/action this file. How is this controlled? How will they be notified action is required (e.g. email, routing slip, etc.)?
- Note the expected timeline for completion (e.g. a license may be issued on the same day while a client may be enrolled in a program for an extended period of time).
- Identify any known deviations from the regular course of business and the required response (e.g. application form is incomplete – return to applicant with memo).
- What event closes the file (e.g. claim is processed, payment issued, project closed, client leaves the program)? File closure typically starts the retention period. Employees may need to notify a manager or IM contact when this event has occurred, or a system report may be used to track closure).
- What steps are required to close the file (e.g. data entry, final file assembly, removal of transitory records, report update, complete checklist, seal file, etc.)?
- If there are multiple records that are required to complete the file, create a checklist for employees to verify that all requirements are met. Review and sign-off of this checklist may be a part of the closure process.

Required Content: Based on the process, what information is typically needed in the case file to meet the public body's legal or operational requirements (e.g. provision by the applicant of a certificate or permit is required by the inspector to complete the assessment)? A checklist may be helpful in ensuring file content is complete. Sample content of a case file may include but is not limited to:

- | | | |
|----------------------------|------------------------|----------------------|
| — Client Application Forms | — Correspondence | — Receipts |
| — Service Requests | — Meeting Agenda/Notes | — Requirements |
| — Assessments/Reports | — Decision Notes | — Invoices |
| — Note to File | — Complaints | — Records of Payment |

Records Creation:

- Forms and templates encourages creation of consistent, complete and accurate records.
- File content may be in a variety of formats: physical and electronic (e.g. file in the registry, data in a system, folder on the network). Identify the technology solutions used to create the case file (e.g. data from the applicant may be entered into a system).
- What information needs to be recorded to manage the file? This information may be tracked manually or in case management system. Information may include but not limited to:
 - o File Number or Unique Identifier (e.g. file number generated by a system, applicant name, project title, etc.)
 - o Relevant dates (e.g. Opened, Actioned, Payment, Closed, etc.)
 - o Names (Internal or external e.g. claimant, employee, vendor, etc.)
 - o Additional process-specific requirements as identified by the process manger

Organization and Storage:

- Identify how individual records, file folders, etc. are to be named/labelled.
- Identify the format and/or location of the final case file (e.g. HPRM EDRMS, File Registry, Network Drive, and Onsite Records Storage).
- Linkages between files should be noted if relevant (e.g. family members enrolled in a program may be linked to a legal guardian).
- Access restrictions and controls must be enforced to protect personal and confidential information.
- Large files may require multiple volumes (e.g. by year) or sub-files (e.g. by record type).

Sharing and Use:

- Consider procedures to track, use and update the file (e.g. routing slip, file inventory slip, system data, and sign in/out procedure).
- Ensure case files are accessible to authorized individuals.
- Provide guidance on how files are to be transferred to another location, or shared with authorized persons (e.g. encrypted email vs. use of interoffice mail vs. Canada Post vs. courier).

Disposal:

Disposal of a case file is permitted when the public body has fulfilled its legal retention requirements.

- Disposal must comply with the Management of Information Act (MOIA).
- Disposal means either secure destruction, transfer to The Rooms Provincial Archives or in rare cases permanent retention by department.
- A disposal authority approved by the Government Records Committee (GRC) is required to dispose of a government record.
- The OCIO supports the Corporate Records and Information Management Standard (CRIMS) for disposal of corporate records.

- Public bodies should reference internal Records Retention and Disposal Schedules (RRDS) for authorization of any additional or specific processes.
- Guidance should outline what information needs to be retained in the final file as a government record versus information considered as transitory as defined in the MOIA (e.g. retain final versions, eliminate copies, file emails and delete from Outlook, etc.).

For additional information on managing records, contact the public body's Information Management Division. General inquiries may be forwarded to IM@gov.nl.ca.

Supporting Materials

Management of Information Act

<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Corporate Records and Information Management Standard

https://www.ocio.gov.nl.ca/ocio/im/c_rims.html

Records Retention and Disposal Schedule Standard

<https://www.ocio.gov.nl.ca/ocio/im/disposal.html>

Government Records Committee

<https://www.ocio.gov.nl.ca/ocio/im/committee.html>

FYI—Identifying and Disposing of Government Records

<https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/governmentrecords.pdf>

FYI—Identifying and Disposing of Transitory Records

<https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/transitoryrecords.pdf>

What is Case Management?

<https://www.aiim.org/What-is-Case-Management>

OCIO website

<https://www.ocio.gov.nl.ca>

Version History

(OCIO Ref. DOC01133/2019)

1.0	2016 08 05
2.0	2019 03 29



FYI

IM Advisory — Executive Records

Overview

This Office of the Chief Information Officer (OCIO) Information Management (IM) Advisory provides common best practices to consider when managing executive records. The audience for this advisory includes all public bodies as defined under the Management of Information Act. Public bodies may develop additional requirements to meet individual needs. Public bodies are advised to consult with their internal IM division to access internal requirements, tools and services. This advisory supplements resources available on the OCIO website.

What are Executive Records?

Executive records include the administrative and operational records of the offices of ministers, deputy ministers, assistant deputy ministers, and equivalent positions. Executive records often document the development, implementation, operation, and evaluation of government legislation, programs, and services. Examples of records or functions may include but are not limited to:

- Briefing Notes
- Cabinet Records
- Communications
- Strategic Planning
- Accountability
- Legislation
- Executive Meetings
- Audit Management
- Committee Records
- Jurisdictional Relations
- Organizational Reports
- Corporate Finance Records

Why Manage Executive Records?

Executive records reflect the overall governance and management of a public body. Some executive functions are led by the executive and therefore have a larger volume of documentation stored within the executive suite (e.g. Organizational Reports). The executive is often engaged in matters that originate with the program-specific lines of business in the public body (e.g., communications related to a new initiative). As a result, the executive provides input to the relevant program or service area. In such instances, government records are retained by the line of business. It is important that executive records are managed effectively because they:

- Provide a complete high-level overview of the public body's fulfillment of its mandate.
- Demonstrate compliance with operational, legal and regulatory requirements.
- Capture senior-level decision making processes.
- May be accessed and scrutinized at a later date by other government employees and members of the public.
- Must be easily accessible to decision makers to:
 - o Maintain operations and the provision of programs and services
 - o Manage and report on resource usage
 - o Respond to issues or inquiries

- Have a high rate of records which may have long-term historical or cultural significance that must be transferred to The Rooms Provincial Archives when the public body has fulfilled legal retention requirements.

Record Characteristics

When creating an executive record, it is important that consideration for inclusion of the following characteristics, if available, are present to ensure that it is complete, authentic and reliable. This information may be recorded within the record or as a part of its metadata:

- | | | |
|----------------|------------------------|---------------------|
| — Date | — Record Type | — Media |
| — Time | — Draft or Final | — Technology Used |
| — Location | — Creator | — Recipient |
| — Participants | — Audience | — Reviewed by |
| — Signatures | — Reference/Identifier | — Alternative Media |

Things to Consider When Managing Executive Records

Employees should have clear direction on how to manage the information used to administer or carry out programs and activities on behalf of the public body. This information may be documented in a training or support manual. Programs or services may have requirements that are unique to the type of information or service as determined by the public body. General considerations when creating information management policies and procedures may include, but are not limited to:

Creation: The OCIO maintains the Corporate Records and Information Management Standard (CRIMS) to provide guidance on the records that may be produced to support executive functions. These examples may be augmented by requirements specific to the public body's mandate (e.g., a Government Department that works closely with the Federal government may participate in Federal, Provincial and Territorial (FPT) working groups).

Cabinet Records: Under the Management of Information Act, Cabinet Records are managed in a manner determined by Cabinet Secretariat. Employees engaged in the cabinet submission process are advised to complete training and remain aware of requirements released by Cabinet Secretariat.

Briefing Materials: There are many types of briefing materials (e.g. executive, departmental, ministerial, etc.). These are described in CRIMS. Cabinet Secretariat has developed new templates to maintain separation between factual information and analysis in briefing materials.

Required Content: For each type of record it is important to ensure that records are complete, accurate and reliable to meet the public body's legal or operational requirements (e.g. report for transparency and accountability meets the needs as specified for the category). Sample content for executive records may include, but is not limited to:

- | | | |
|------------------------|-------------------|---------------------|
| — Memo from Executive | — Correspondence | — Reports |
| — Completed Template | — Meeting Minutes | — Analysis |
| — Supporting Documents | — Decision Notes | — Committee Records |
| — Appendices | — Notes to File | — Legal Opinions |

Roles and Responsibilities: Multiple employees may need to access/action executive records. The management team may consider providing employees with a reference including how information is controlled, and how individuals are notified that an action is required (resulting from this activity).

Technology: All employees must comply with the OCIO's Directive on Acceptable Use of the Government Network and Information Technology Assets. Identify the technology solutions used to support the records' functions:

- Use of Network File Share/Personal file share: Define what records will be stored when, how and by whom for all executive functions.
- USB Flash Drives: Use only encrypted removable media when necessary as per the OCIO's guidance.
- Use of HPRM: HPRM is the government of Newfoundland and Labrador's standard Electronic Document and Records Management System (ERDMS). Public bodies are responsible for their own internal administration of their HPRM installation. HPRM has been implemented as the standard tool to support executive correspondence. Public bodies may determine other record types to use in HPRM to support executive functions.
- Email Management: Compliance with the OCIO's Email Management Policy.
- Instant Messaging: Compliance with the OCIO's Directive on Instant Messaging.
- Mobile Devices: Compliance with the OICO's Directive on Mobile Devices for Government Employees.

Forms/Templates: Use of forms and templates encourages creation of consistent, complete and accurate records.

Transport/Sharing: Identify procedures for how files are to be transferred to another location or shared with authorized persons (e.g. encrypted email vs. use of interoffice mail vs. Canada Post vs. courier). Some files may require specific considerations:

- Cabinet Records
- Budget Documents

Storage: Executive records may have highly-sensitive content. Access restrictions and controls must be enforced to protect personal and confidential information. Records should be stored in physical format in either the executive suite or in a secure location accessible only to authorized employees. Electronic storage, including the network file shares and HPRM electronic document and records management libraries, must apply appropriate access levels.

Naming Conventions/Labelling: Identify how individual records, file folders, etc. are to be named/labelled.

Secure Destruction of Transitory Records: Guidance should outline what information needs to be retained in the final file as a government record vs. what information is considered transitory as defined in the Management of Information Act (e.g., retain final versions, eliminate copies, print emails and file deletions from Outlook, etc.). Ensure that copies of transitory records required by lines of business, including executive input, are securely destroyed.

Disposal: Disposal of executive records is permitted when the public body has fulfilled its legal retention requirements:

- Disposal must comply with the Management of Information Act (MOIA).
- Disposal means either secure destruction, transfer to The Rooms Provincial Archives or in rare cases permanent retention by department.
- A disposal authority approved by the Government Records Committee (GRC) is required to dispose of a government record.
- The OCIO supports the Corporate Records and Information Management Standard (CRIMS) for disposal of corporate records.
- Public bodies should reference internal Records Retention and Disposal Schedules (RRDS) for authorization of any additional or specific processes.
- Guidance should outline what information needs to be retained in the final file as a government record versus information considered as transitory as defined in the MOIA (e.g. retain final versions, eliminate copies, file emails and delete from Outlook, etc.).

For additional information on managing records, contact the public body’s Information Management Division. General inquiries may be forwarded to IM@gov.nl.ca.

Supporting Materials

Version History

Management of Information Act

(OCIO Ref. DOC01134/2019)

<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Policy - Email

1.0 2016 02 04

<https://www.ocio.gov.nl.ca/ocio/email/index.html>

2.0 2019 03 39

Directive - Instant Messaging

https://www.ocio.gov.nl.ca/ocio/instant_messaging.html

Directive - Acceptable Use of the Government Network and Information Technology Assets

https://www.ocio.gov.nl.ca/ocio/im/employees/asset_use.html

Directive - Mobile Devices for Government Employees

https://www.ocio.gov.nl.ca/ocio/publications/policies/Directive_Mobile_Devices_for_Government_Employees.pdf

Corporate Records and Information Management Standard

https://www.ocio.gov.nl.ca/ocio/im/c_rims.html

Records Retention and Disposal Schedule Standard

<https://www.ocio.gov.nl.ca/ocio/im/disposal.html>

Government Records Committee

<https://www.ocio.gov.nl.ca/ocio/im/committee.html>

FYI - IM Advisory - Note to File

https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Note_to_File.pdf

FYI - IM Advisory - Case Files

https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Case_Files.pdf

FYI – Information Protection – USB Drives – What You Should Know

https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/FYI_Information_Protection-USB_Drives.PDF




FYI

IM Advisory — Meeting Records

Overview

This Office of the Chief Information Officer (OCIO) Information Management (IM) Advisory provides common best practices to consider when managing meeting records. The audience for this advisory includes all public bodies as defined under the Management of Information Act. Public bodies may develop additional requirements to meet individual needs. Public bodies are advised to consult with their internal IM division to access internal requirements, tools and services. This advisory supplements resources available on the OCIO website.

What are Meeting Records?

Meeting records include all information that is used to organize, manage and document a meeting. A meeting is an assembly or conference of two or more persons organized for a specific purpose or to meet ongoing management requirements. Meeting records often document decisions related to government programs and services. Examples of meeting records may include:

- Agendas
- Handouts
- Correspondence
- Presentations
- Minutes
- Informal Notes
- Invitations
- Whiteboard Content
- Meeting Records

Why Manage Meeting Records?

Meeting records are used to direct action, make decisions and track progress. Meeting records may include information about events, discussions and decisions not found elsewhere. Personal judgment is often required of participants to ensure records are adequate. It is important that these records are managed because:

- Meeting records are used to identify issues, disseminate information, document analysis and assign/track actions necessary to demonstrate due diligence in policy development or decision making. This information may be required for reference, operationally or for legal purposes.
- Meeting records provide a consistent structure around the meeting process thereby supporting the creation and retention of information.
- Meeting management may reduce the creation, retention and management of transitory records. For example, if participants agree that one attendee will create, circulate and finalize minutes then the practice of multiple attendees recording their own interpretation of the discussion will be discontinued. This results in a clearer, more complete record of events that is agreed upon. Participants will have confidence that copies of notes, agendas and draft minutes can be securely disposed of because the official final version is being managed.

Record Characteristics

When creating a meeting record, it is important that consideration for inclusion for the following characteristics, if applicable, are noted to ensure the record is complete, authentic and reliable. This information may be recorded within the record or as a part of its metadata:

- | | | |
|------------|------------------------|-----------------------|
| — Date | — Record Type | — Media |
| — Time | — Draft of Final | — Technology Used |
| — Location | — Meeting Chair | — Recipient |
| — Regrets | — Minute Taker | — Reviewed by |
| — Invitees | — Reference/Identifier | — Document Circulated |

Things to Consider When Managing Meeting Records

Employees should have clear direction on how to manage information used to administer or carry out programs and activities on behalf of the public body. This information may be documented in a training or support manual. Programs or services may have requirements that are unique to the type of information or service as determined by the public body. General considerations when creating information management policies and procedures may include, but are not limited to:

Considerations should be made to document:

- Standing Meetings including team or management meetings where direction is provided, work is assigned or information is communicated to employees should include an agenda and minutes.
- Committee Meetings including standing committees (financial management, occupational health and safety, etc.), working groups or ad hoc committees should retain meeting records.
- Meetings that monitor the implementation of a project.
- Meetings organized to deal with an issue or initiative.

Unscheduled or informal meetings:

Not all meetings may require the same level of detail in organization, tracking and documentation. If a meeting is unscheduled then an agenda will not exist and it will be at the discretion of the participants to determine whether documentation is needed. A summary of the discussion or action items may be sufficient to ensure a common understanding of decisions or action items needed. A note to file (see advisory: note to file) may be sufficient in the event that issues were identified or decisions made that need to be added to a file but do not need to be communicated back to the participant. At the end of the meeting the employee in the senior role should assume or assign this responsibility as appropriate.

Purpose/Planning:

What is the requirement, issue or event that drives the meeting? Defining the purpose or objectives and goals will determine who the optional or mandatory attendees are. What content will be reviewed? Is there information that will be distributed before, during or following the meeting.

Agenda: An agenda is a core meeting record. Prepare the agenda based on the planning effort. Content may include:

- Date, time and location
- Attendees and status – mandatory or optional
- Topics for discussion/content – identify the lead participant. If multiple topics are planned setting a time for each topic based on level of priority or anticipated effort may be helpful in keeping the meeting on track. If the meeting is recurring the first agenda item may be to approve the minutes from the previous meeting.

Roles and Responsibilities: Assign roles and responsibility for managing information to one participant. This is particularly important when there are a number of attendees. This would include assigning someone to:

- Create meeting
- Arrange room
- Setup online requirements
- Create /distribute agenda
- Track attendees
- Arrange building security
- Take Minutes
- Circulate minutes

At the start of the meeting communicate to participants how the meeting will be managed.

Media: Meetings may be facilitated in person, over the telephone or through online meeting technology such as Skype for Business. Recording options may vary depending on the type of meeting.

Forms/Templates: Use of forms and templates encourages creation of consistent, complete and accurate records. See above record characteristics for elements to consider.

Minutes/Notes: Points to consider when creating these records:

- Meeting minutes typically include the same information as included in the agenda. You may use the agenda, if one exists, as a guide to create the minutes.
- If a sign-in sheet is not used, check off attendee names as they enter the meeting either physically or online.
- Meeting minutes are not intended to be a transcript of a discussion. Minutes document discussion points, decisions, and required actions as well as to whom they are assigned and known timelines.
- Request clarification in the event a statement, decision or discussion point is not clear.
- Generally minutes do not attribute statements to an individual unless requested. This should be stated at the start of the meeting as a part of the terms of reference.
- Creating minutes electronically as they occur is recommended where possible. If this is not possible, create minutes as soon as possible following the meeting.

Storage: Meeting records should be stored within the context of the project, program, service, etc. to which they relate. Store meeting records together as a package (e.g., all documents related to the meeting including the agenda, minutes, presentations, handouts, etc.) by meeting date.

Protection: Ensure that safe meeting practices are followed particularly when sensitive matters are discussed:

- Book a meeting room instead of crowding around an individual’s desk or meeting in a public area (e.g. cafeteria, coffee shop, etc.).
- Close doors if sensitive matters are being discussed.
- Pause the meeting when a non-participant enters the room (e.g., support staff, audio-visual support staff, caterers, etc.)
- Erase all whiteboards at the conclusion of the meeting.
- Collect all papers from the room before leaving and deposit in the secure shred bin instead of the recycle bin or garbage.

Disposal: Disposal of meeting records is permitted when the public body has fulfilled its legal retention requirements.

- Disposal must comply with the Management of Information Act (MOIA).
- Disposal means either secure destruction, transfer to The Rooms Provincial Archives or in rare cases permanent retention by department.
- A disposal authority approved by the Government Records Committee (GRC) is required to dispose of a government record.
- The OCIO supports the Corporate Records and Information Management Standard (CRIMS) for disposal of corporate records.
- Public bodies should reference internal Records Retention and Disposal Schedules (RRDS) for authorization of any additional or specific process for meeting records.
- Guidance should outline what information needs to be retained in the final file as a government record versus information considered as transitory as defined in the MOIA (e.g. retain final versions, eliminate copies, file emails and delete from Outlook, etc.).

For additional information on managing records, contact the public body’s Information Management Division. General inquiries may be forwarded to IM@gov.nl.ca.

Supporting Materials

Version History

- Management of Information Act*
<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>
- Corporate Records and Information Management Standard
https://www.ocio.gov.nl.ca/ocio/im/c_rims.html
- Records Retention and Disposal Schedule Standard
<https://www.ocio.gov.nl.ca/ocio/im/disposal.html>
- Government Records Committee
<https://www.ocio.gov.nl.ca/ocio/im/committee.html>
- FYI - IM Advisory - Note to File
https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Note_to_File.pdf
- OCIO website
<https://www.ocio.gov.nl.ca>

(OCIO Ref. DOC01136/2019)

1.0	2016 02 04
2.0	2019 03 29





IM Advisory — Note to File

Overview

This Office of the Chief Information Officer (OCIO) Information Management (IM) Advisory provides common best practices to consider when managing a note to file. The audience for this advisory includes all public bodies as defined under the Management of Information Act. Public bodies may develop additional requirements to meet individual needs. Public bodies are advised to consult with their internal IM division to access internal requirements, tools and services. This advisory supplements resources available on the OCIO website.

What is a Note to File?

Note to file is an independent recording of an event, situation or observation. The use of note to file is common in many professions and industries. It is a way to document information that is either observed or transmitted verbally and therefore not recorded via the tools, systems, forms and templates that support the process. While the term “note to file” may not be used by employees, many processes or services create a record where information would not be captured either electronically (e.g. system data) or through process specific documentation (e.g. application form). In some practice areas, a note to file may be part of the standard operating procedure (e.g., a clinician creates a note when a client’s condition changes). Other instances may be based on the judgment of the employee (e.g. an employee creates a note in a client file that they have left three voice messages with no response). Examples of events or situations that may prompt the employee to create a note to file include:

- Client Interactions
- Conversations
- Workplace Incidents
- Medical Events
- Instant messages
- Research Results
- Telephone Calls
- Observations
- Test Results
- Information Meetings
- Independent Decisions
- Complaints

Why Manage a Note to File?

The Management of Information Act requires that all public bodies retain records reflective of their mandate. A note to file may have a significant impact on the provision of a program or service. Information contained within the note may not be available elsewhere and may be critical to the public body’s decision making rationale. A note to file is a helpful tool used to record everything from procedural discrepancies to the physical location of files. If you need to keep track of everything from major details about a client to seemingly minor issues, learning how to write a note to file is important. For example, if someone calls or sends you an email asking you to make a change to a plan or alter a course of action, write a note to file in case another party later questions your actions. Notes to file are important for legal, medical or other highly sensitive files

that might later be used in court as well. Notes to file generally:

- Are generated on a case-by-case basis.
- Include the subject (if applicable).
- Are signed and dated by the individual who is writing it.
- Are legible if handwritten.
- Explain clearly and specifically the reason for the error/omission/discrepancy or process/policy it aims to address. Avoid using “one-size-fits-all” notes when providing details. Overuse of a blanket statement will take away from the value of a note to file.
- Include any corrective action or follow-up when applicable.
- Are filed with the document or file to which it relates.
- Are an accurate reflection of the occurrence (Provide sufficient detail to aid understanding of the occurrence.)
- Are created as soon as possible following the occurrence that initiates it.

Record Characteristics ---

When creating a note to file, it is important that consideration for inclusion of the following characteristics, if available, are present to ensure that it is complete, authentic and reliable. This information may be recorded within the record or as a part of its metadata:

- | | | |
|------------------------|-------------------------|-------------------------|
| — Date of Occurrence | — Subject or Process | — Action Planned/Taken |
| — Location/Media | — Identify File Linkage | — Name of Note Creator |
| — Names of Individuals | — HPRM Reference # | — Signature of Creator |
| — Time | — Date of Note | — Summary of Occurrence |

Things to Consider When Managing Meeting Records ---

Employees should have clear direction on how to manage the information used to administer or carry out programs and activities on behalf of the public body. This information may be documented in a training or support manual. Programs or services may have requirements that are unique to the type of information or service as determined by the public body. General considerations when creating information management policies and procedures may include, but are not limited to:

Creation Trigger:

Identify events or incidents that may require a note to file to demonstrate for employees that this practice is acceptable and required:

- There may be industry or professional process requirements where notes are required.

- Note to file may require employees to use judgement in determining when to create a note to file. Providing examples wherever possible of events or situations that may necessitate a note to file may be helpful in assisting employees to apply this requirement more effectively.

Professional Standards:

Identify any professional or industry standards related to the program or service when creating a note to file.

Technology:

Identify the technology solutions used to support the process (e.g. a field or form in the case management system is available to create note to file).

Forms/Templates:

Use of forms and templates encourages creation of consistent, complete and accurate records.

Creation Media:

Identify the media in which the note is best created (e.g. system field, Microsoft Word, paper record).

Handwritten Notes:

Handwritten notes must be legible. Also, there may be a requirement to use either pencil or ink to create the note based on the process or industry.

Context:

Note to file must be retained and accessible within the context of the business process. Management requirements are defined in Operational Records Retention and Disposal Schedules and in the Corporate Records and Information Management Standard (CRIMS).

Storage:

Identify where and how the note to file is to be stored (e.g. in a case file, on a Network Drive, etc.).

Disposal:

Disposal of a note to file is permitted when the public body has fulfilled its legal retention requirements:

- Disposal must comply with the Management of Information Act (MOIA).
- Disposal means either secure destruction, transfer to The Rooms Provincial Archives or in rare cases permanent retention by department.
- A disposal authority approved by the Government Records Committee (GRC) is required to dispose of a government record.

- The OCIO supports the Corporate Records and Information Management Standard (CRIMS) for disposal of corporate records.
- Public bodies should reference internal Records Retention and Disposal Schedules (RRDS) for authorization of any additional or specific process for meeting records.
- Guidance should outline what information needs to be retained in the final file as a government record versus information considered as transitory as defined in the MOIA (e.g. retain final versions, eliminate copies, file emails and delete from Outlook, etc.).

For additional information on managing records, contact the public body’s Information Management Division. General inquiries may be forwarded to IM@gov.nl.ca.

Supporting Materials

- Management of Information Act*
<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>
- Corporate Records and Information Management Standard
https://www.ocio.gov.nl.ca/ocio/im/c_rims.html
- Records Retention and Disposal Schedule Standard
<https://www.ocio.gov.nl.ca/ocio/im/disposal.html>
- Government Records Committee
<https://www.ocio.gov.nl.ca/ocio/im/committee.html>
- FYI - IM Advisory - Case File Management
https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Case_Files.pdf
- OCIO website
<https://www.ocio.gov.nl.ca>

Version History

(OCIO Ref. DOC01137/2019)

1.0	2016 02 04
2.0	2019 03 29



FYI

IM Advisory — Program Administration Records

Overview

This Office of the Chief Information Officer (OCIO) Information Management (IM) Advisory provides common best practices to consider when managing program administration records. The audience for this advisory includes all public bodies as defined under the Management of Information Act. Public bodies may develop additional requirements to meet individual needs. Public bodies are advised to consult with their internal IM division to access internal requirements, tools and services. This advisory supplements resources available on the OCIO website.

What are Program Administration Records?

A program is a group of related, functions, activities, projects or services delivered by a public body to meet legislative, accountability, administrative or service commitments. Programs feature a hierarchy of management, ongoing funding, dedicated resources and well-defined deliverables or commitments. Program administration refers to activities required to plan, develop, deliver and monitor a program. Program records document the overall management of the program including the foundation, mandate, resource usage and performance.

While the term “program administration” may not be used, most government processes can be linked to a program. Examples of program administration records may include but are not limited to:

- Forms and Templates
- Management Meetings
- Policies and Procedures
- Program Planning
- Vision Statement
- Statistics
- Program Evaluations
- Agreements and Contracts
- Copies of Legislation
- Benchmarks
- Mission Statement
- Associations and Conferences
- Orders and Directives
- Reports
- Team Meetings
- Working Groups
- Guiding Principles
- Works Plans

Program administration records are typically managed by the employee responsible for the program (program manager). The records of the program (e.g., project files, case files, service records, etc.) are not included as program administration records.

Program administration records fall into three categories:

1. **Strategic Planning and Reporting:** Includes records related to the program’s establishment, mandate and reporting requirements. These records must be retained internally for reference by the management team until superseded or obsolete.

FYI — IM Advisory — Program Administration Records

2. **Ongoing Management:** Includes records related to operational planning, assignment of tasks and interactions with stakeholders and team members. A large volume of day to day operations may be transitory. Records of enduring value in this group must be retained internally for reference by the management team until superseded or obsolete.
3. **Transitory Records:** A large volume of program administration records may be copies of records retained by another office (e.g., Human Resource Secretariat (HRS) will retain HR records, Department of Finance will retain payroll records, the Executive Suite will retain organizational planning, reporting, cabinet records, etc.). It is the responsibility of the employee in charge of the program to dispose of transitory records as appropriate.

Why Manage Program Administration Records?

A senior manager is typically responsible for program administration. This employee works within the regulatory and administrative framework of government to manage the resources required to maintain the program. Programs may relate to either corporate or administrative functions (e.g., Finance, Human Resources, etc.) or to a public body's unique mandate (e.g., Public Services). Because of this, the program manager may retain copies of records that are held by other offices (e.g., Copies of Payroll reports from Human Resources).

Program administration may have a high rate of records having long-term historical or cultural significance that must be transferred to The Rooms Provincial Archives when the public body has fulfilled legal retention requirements. They are an important reference point for the management team to ensure:

- Resources are coordinated and appropriately assigned to work.
- Corporate memory of the program, its mandate, strategic direction and performance are retained and available for future planning.

Record Characteristics

When creating a meeting record, it is important that consideration for inclusion for the following characteristics, if applicable, are noted to ensure the record is complete, authentic and reliable. This information may be recorded within the record or as a part of its metadata:

- | | | |
|------------------------|-------------------------|------------------------|
| — Record Type | — Subject or Process | — Governance |
| — Location/Media | — Identify File Linkage | — Record Creator/Owner |
| — Names of Individuals | — HPRM Reference # | — Signature of Creator |
| — Signing Authority | — Last Update | — Dates of Relevance |

Things to Consider When Program Administration Records

Employees should have clear direction on how to manage the information used to administer or carry out programs and activities on behalf of the public body. This information may be documented in a training or support manual. Programs or services may have requirements that are unique to the type of information or service as determined by the public body. General considerations when creating information management

policies and procedures may include, but are not limited to:

Creation: Program administration requirements may be defined by central administrative functions (e.g., Finance, HRS) or driven by a public body's unique mandate. Program managers should have a good understanding of the records required to support and document the processes for which they are responsible and be able to direct employees as necessary. For administrative functions, the project manager will be required to follow the requirements defined by central administrative functions. If the program is unique, the program manager should define and communicate the record creation requirements.

Organization: Efficient organization and storage of program records is recommended for access and disposal management. Implementing a file classification plan, as described in the OCIO guidelines: Classification Plan Development and Classification Plan Implementation is recommended. One option would be to organize records by the record types provided in the examples above and the year or date. Consistent file labelling and record naming conventions should be defined, communicated and followed by all employees.

Forms and Templates: The use of forms and templates encourages creation of consistent, complete and accurate records. The program manager will be required to adhere to forms and templates issued by central administration. The program manager may also oversee the development of internal forms and templates to support program requirements. The location of updated forms and templates should be communicated to employees as a part of policies and procedures.

Meeting Records: The program manager will maintain meeting records to document the operation of the program. In addition to internal team meetings, meetings with stakeholders may be required. See the OCIO IM Advisory - Meeting Records for detailed guidance.

Policies and Procedures: Policies and procedures direct employees on how to deliver the program. These may include what records need to be created to support the program and associated management requirements. These may be provided by a central function or developed internally by the program manager.

File Format: Records may be in a variety of formats including physical and electronic (e.g. file in the registry, data in a system, databases, folder on network). The program manager should have an understanding of all records and their formats. Identify the format and location of the final records (e.g., HPRM EDRMS, File Registry, Network Drive, and Records Storage).

Storage: Employees working within the program may require access to some program records while others may need to be restricted due to sensitivity of content. Where to store program records should be documented in employee policies and procedures. The program manager must maintain records with sensitive information in a secure location (e.g., Secure Network Drive or locked workstation cabinet/drawer).

Ownership: Program managers must have a clear understanding of which records need to be retained by the program versus which are copies of records retained by another public body or organizational group. This is particularly important for corporate or administrative records whereby a complete set or portion of the records may be forwarded to an other department (e.g., Finance, HRS).

Secure Destruction of Transitory Records: Program administration often includes activities that are routine or of minor importance but required to facilitate administration (e.g., booking meetings, receiving updates from the central administrative unit, etc.). Transitory records must be securely destroyed as per the Management of

Information Act as a regular course of business. This includes copies of records that are retained by another department or public body (e.g., Finance, HRS).

Disposal: Disposal of program administration records is permitted when the public body has fulfilled its legal retention requirements.

- Disposal must comply with the Management of Information Act (MOIA).
- Disposal means either secure destruction, transfer to The Rooms Provincial Archives or in rare cases permanent retention by department.
- A disposal authority approved by the Government Records Committee (GRC) is required to dispose of a government record.
- The OCIO supports the Corporate Records and Information Management Standard (CRIMS) for disposal of corporate records.
- Public bodies should reference internal Records Retention and Disposal Schedules (RRDS) for authorization of any additional or specific processes.
- Guidance should outline what information needs to be retained in the final file as a government record versus information considered as transitory as defined in the MOIA (e.g. retain final versions, eliminate copies, print emails and delete files from Outlook, etc.).

For additional information on managing records, contact the public body’s Information Management Division. General inquiries may be forwarded to IM@gov.nl.ca.

Supporting Materials

Version History

- Management of Information Act*
<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>
- Corporate Records and Information Management Standard
https://www.ocio.gov.nl.ca/ocio/im/c_rims.html
- Records Retention and Disposal Schedule Standard
<https://www.ocio.gov.nl.ca/ocio/im/disposal.html>
- Government Records Committee
<https://www.ocio.gov.nl.ca/ocio/im/committee.html>
- FYI - IM Advisory - Meeting Records
https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Meeting_Records.pdf
- Guideline - Information Management Program Plan
https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Note_to_File.pdf
- Guideline - Classification Plan Development for Operational Records
https://www.ocio.gov.nl.ca/ocio/im/practitioners/guideline_docs/3_2_Classification_Plan_Development.pdf
- Guideline - Records Classification Plan Implementation
https://www.ocio.gov.nl.ca/ocio/im/practitioners/guideline_docs/3_3_Classification_Plan_Implementation.pdf

(OCIO Ref. DOC01138/2019)

1.0	2016 02 04
2.0	2019 03 29



Overview

Records transferred to offsite storage must be carefully organized and documented to ensure future accessibility. For more information on preparing records for offsite storage, contact IM@gov.nl.ca.

General Advice

- Perform an initial assessment of the records:
 - Identify each records series to be transferred. Remember to record the Records Retention and Disposal Schedule (RRDS) title and number, where appropriate.
 - Verify the department is the Office of Primary Responsibility (OPR) for the records.
 - Records that have met retention requirements are ready for disposal. This means either transfer to The Rooms Provincial Archives Division or secure destruction if records are deemed to have no archival value.
- Identify a location where records can be processed. Consider:
 - A large table where records can be organized, foldered and labeled.
 - Access to equipment (e.g. computer and printer to create and print labels).
 - Secure shredding bins to securely destroy transitory records.
 - Ability to secure records during off hours/while awaiting pickup.
- Determine where records will be stored:
 - Certain government records are eligible for storage at the PRC at no cost to the department. Refer to the IM Advisory [Transferring Records to the Provincial Records Centre](#).
 - The Rooms Provincial Archives will accept records that have been pre-approved by the Government Records Committee (GRC) of having the disposition of Archive or Selective Retention on the RRDS. This is typically a very small volume of records, 5% - 10%. Consult with the [Government Records Archivist](#) on how to transfer records to the Rooms Provincial Archives.
 - Third party storage is used for the largest volume of government records. Each department pays for the storage of their own boxes. Contact the Government Purchasing Agency for a master standing offer agreement for this service.
- Use only standard size boxes procured via the master standing offer agreement for boxes. This box type fits on standard shelving.
- Seal the box with packing tape to minimize risk to records while in transit.

Advice continued.....

- Organize records that will go into each box:
 - Arrange records according to the departmental filing system (e.g. numerical, alphabetical, and chronological). Retain any internal file listings or finding aids, as these will be useful in mapping records to the RRDS.
 - Securely destroy any transitory materials including duplicate copies, published materials, etc.
 - Eliminate metal bindings, as this will make the box lighter and protect records as metal corrodes over time.
 - Store records in labeled folders, as this supports a faster, more secure retrieval.
 - Do not use hanging file folders, as these folders destroy the box over time.
 - Pack only one type of record series per box with a similar disposal date. Retention requirements for a series may change over time. If there are multiple series in a box then changes may require re-boxing and re-indexing the records.
- Document each box with a file list that itemizes content.
 - The level of detail may vary (e.g. case files may require an alphabetical list of names while a date range may be sufficient for records filed chronologically); however it must be sufficient to enable future retrieval of the records.
 - A sample file listing template is on the OCIO website as the second page of the [Record Transfer form](#).
 - Calculate a disposal date based on the RRDS (e.g. records from September 2012 with 5-year retention in the semi-active column will be disposed of in September 2017).
- Boxes should be packed leaving a 1-2 inch gap to allow for easier access when doing retrievals.
- Each box must have a departmental box number that corresponds to the department's inventory listing.
- Do not put any other markings on the box that reveal the content of the records. Boxes will be assigned tracking numbers that correlate to the records transfer forms.

Overview

The Provincial Records Centre (PRC) is operated by the Office of the Chief Information Officer (OCIO). The PRC provides secure storage for semi-active government records that fall within its mandate. A complete and accurate [Request for Records form](#) is required to process all retrievals. Contact the PRC at 709-729-3628 or grlm@gov.nl.ca for information on request for records.

General Advice

- A *Provincial Records Centre (PRC) Client Chart of Authority* must be established in order for a department to request records from the PRC. For further information on Chart of Authorities contact grlm@gov.nl.ca.
- Always use the updated Request for Records form located on the OCIO website: [Provincial Records Centre](#).
- Forms must be completed electronically. Handwritten forms are not accepted.
- Complete one form for all records requested, unless the shipping address is different.
- All sections of the form must be completed correctly.
 - PRC staff will not change forms on the requester's behalf. If it is determined that a form contains incorrect information, a requester will be asked to re-submit the request.
- Forward completed forms to the PRC via email to GRLM@gov.nl.ca.
- Improper labeling of records by the department at the time of storage may cause a processing delay.
- Records are shipped by the PRC via:
 - Internal Mail: Locations serviced by internal mail system, 1-2 business days.
 - Xpresspost: Locations not serviced by internal mail, 3-5 business days.
 - Courier: PRC will notify the requester via email the size and weight of records so that they may arrange pickup. Requester must arrange for courier to pick up records.
- Time of shipment from the PRC is dependent on the time of day the request is received/processed.
- Custody of the records is assigned to the requester in the PRC's tracking system.
- It is the requester's responsibility to:
 - Track the records once they are received;
 - Review records for completeness prior to return to the PRC; and
 - Coordinate return of records to the PRC.

Completing the *Request for Records Form***Part 1- Requestor Information**

- Requested By/Department/Public Body/Branch: Identify who has ownership and responsibility for the records.
- Address of Requester/Email/Phone: Contact information for the employee requesting the records.
- Date of Request: Date that the request is sent to the PRC.

Part 2 - Shipping Information

- Only complete this section if the information is different than the above Requestor's Information.
- Name/Department/Public Body/Branch/Email/Phone: Identify the employee that will receive/use the records (e.g. departments may assign an employee to coordinate records retrieval).
- Shipping Address / Shipping Method: Identify the location where the records must be shipped and identify the urgency of the request and method of delivery.

Part 3 - Nature of Request

- Temporary Loan/Permanent Withdrawal: Must indicate one of the two options.
 - Temporary loans must be returned within 30 days. It is the responsibility of the requester to notify the PRC in the event that records are required for a longer period of time. Records not returned within the 30 day period will be signed out permanently to the department.
 - PRC must be aware of permanent withdrawals to enable use of empty storage and to update record status in the tracking system.

Part 4 – Request Details:

- Box or File: Identify whether the request is for the complete box or an individual file.
- Records Series Title/File Title: Describe the box/file. This information is located on the records transfer list which was completed by the department when the records were transferred to the PRC.
- Departmental Box Number: The unique identifier assigned by the department prior to the transfer to the Provincial Records Centre.
- Provincial Records Centre (PRC) Location: The unique location number assigned by PRC employees. This location number is provided to departments when records are transferred to the PRC.

Overview

The Provincial Records Centre (PRC) is operated by the Office of the Chief Information Officer (OCIO). It provides secure storage for the following classes of scheduled semi-active Government records:

- Vital Records that are identified as either indispensable to a mission critical business operation or essential for the continuation of an organization during or following a disaster.
- Records for which the legal or operational needs of the department dictate that custody and/or control of the information must remain within government.
- Records which, due to their enduring value or historical significance, are to be transferred to The Rooms Provincial Archives Division when no longer required by the department or public body.
- Records which have longer than usual semi-active retention periods may be considered, to lessen the burden of storage costs on departments and public bodies.

A [Request Transfer Form](#) must be completed when transferring records to the Provincial Records Centre (PRC). This ensures that all records are captured appropriately, detailing the retention and disposition schedule and any unique identifiers to facilitate retrievals. Contact the PRC at 709-729-3628 or grlm@gov.nl.ca for information on record transfers.

General Advice

- Consult with PRC staff before beginning the transfer process to:
 - Verify that records fall within the PRC mandate.
 - Ensure space is available for storage. Note that an individual transfer must not exceed 100 boxes.
 - Schedule a date for transfer.
 - Establish a *PRC Client Chart of Authority* for access to records.
- Records must be boxed as per the *IM Advisory [Preparing Paper Records for Offsite Storage](#)*.
- Ensure boxes awaiting transfer are locked in a secure location.
- Engage a reputable vendor to physically transfer records. Accompany vendor while boxes are loaded and verify that security measures will be in place during transit.
- Forward completed forms to the PRC via email to GRLM@gov.nl.ca prior to transfer to ensure acceptability and to confirm shipment date/time.
- PRC staff will process boxes as they arrive. This includes:
 - Entering transfer information for each box into the PRC tracking system.
 - Allocating a shelf location to each box.
 - Recording storage details on the transfer form for each box. A copy of the transfer forms will be returned to the departmental contact responsible for the transfer. These forms should be retained to facilitate any future retrieval requests.

Completing the Records Transfer Form

- Always use the updated Records Transfer form located on the OCIO website: [Provincial Records Centre](#).
- Forms must be completed electronically. Handwritten forms are not accepted.
- A complete and accurate records transfer form must accompany each box.

Part 1 - Records Centre Use Only

- This section of the form is completed by PRC staff, and returned to the department.
- This section will include tracking and location information required by the department to request records in the future.

Part 2 - Departmental Information:

- Department/Public Body/Branch/ Address: Identify the organization and unit that is responsible for the records.
- Records Custodian/Email/ Phone Number: Identify the name and role of the employee responsible for the records.
- Requestor Name/Email/Phone Number: Identify the employee that has initiated the transfer. This may be different from the records custodian.
- Record Series Title: Use the title assigned on the department's relevant Records Retention and Disposal Schedule (RRDS).
- Schedule Number: Identified on the RRDS.
- File Date Range: Review the dates contained with the box as identified on the file list.
- Disposal Date: Calculate this date based on the date of the records and the instructions on the RRDS. The PRC will not accept records without a disposal date.
- Departmental Box Number: The unique identifier assigned by the department for its own tracking purposes.

Part 3 - Records Transfer List

- The top section of this form will be populated from the fields in page one of the form above.
- Dates of records: Indicate the date range in the YYYY-MM-DD format.
- File Title: Provide a detailed list of file titles. It is important that box contents can be matched accurately to this listing in the event that the department requests access to an individual file.
- File Numbers: Identify specific file numbers (if applicable).



8. F.A.Q

- 8.1. Acceptable Use of Government Network and/or IT Assets
- 8.2. Information Management and Protection Policy
- 8.3. Instant Messaging
- 8.4. Use of Non-Government Email Accounts for Work Purposes
- 8.5. Corporate Records Information Management Standard (C-RIMS)
- 8.6. Records Retention and Disposal Schedule
- 8.7. One Time Disposal
- 8.8. Government Records Committee
- 8.9. Provincial Records Centre

Acceptable Use of the Government Network and/or IT Assets

FAQs for Employees

What is the OCIO's Acceptable Use Directive?

The Office of the Chief Information Officer's (OCIO) 'Acceptable Use Directive' provides a list of activities and actions that Employees must follow in order to maintain the security and performance of the Government Network and Government's IT assets. This Directive gives OCIO the authority to respond accordingly to threats that may impact the security and performance of the Government Network and/or IT assets. The focus of this Directive is network security and performance – for information on acceptable Internet usage, read the 'Equipment and Resources Usage Policy' in the Human Resources Policy Manual -

http://www.exec.gov.nl.ca/exec/pss/working_with_us/equipment_and_resources.html.

Does this Directive apply to me?

The OCIO's Acceptable Use Directive applies to all Government departments and public bodies supported by the OCIO; it is mandatory for all Employees to follow. Employees, in this context, applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons entrusted to access or use the Government Network and/or IT assets.

Why do I need to protect the Government Network and IT Assets?

Failure to properly protect and maintain the performance of the Government Network and IT assets may impact Government's ability to deliver its services to citizens, employees and businesses by compromising the availability and functionality of Government's electronic systems. Failure to protect the security of the Government Network and IT assets could also result in a breach of Government, citizen and/or business information. As 'Information Protection is Everyone's Responsibility', all employees have an obligation to protect the Government Network and any IT assets in their use.

How do I protect the Government Network and IT Assets?

Protecting the Government Network and IT assets is the responsibility of all employees; whether at work or away from the office, you can do your part to protect the Government Network and IT assets by following the guidance and advice available on OCIO's website - <https://www.ocio.gov.nl.ca/>. In particular, OCIO points you to the following:

- ***IP in the Workplace – Top Tips for Protecting Government Information***
[https://www.ocio.gov.nl.ca/ocio/im/practitioners/Information_Protection_IP_in_the_Workplace_\(Top_Tips\).pdf](https://www.ocio.gov.nl.ca/ocio/im/practitioners/Information_Protection_IP_in_the_Workplace_(Top_Tips).pdf)
- ***Cyber Security – How to Protect Against Cyber Attacks***
<https://www.ocio.gov.nl.ca/ocio/security/cybersecurity.html>
- ***Password Management Best Practices***
http://www.ocio.gov.nl.ca/ocio/im/employees/pdf/password_management_bp.pdf); and

Employees are also strongly encouraged to complete the online ***Cyber Security Awareness e-Learning Module***, which is accessible through Government's Learning Management System, PS Access. This short and simple e-learning module helps employees understand the important role they play in recognizing cyber threats and taking action to prevent cyber-attacks to the Government Network and its IT devices. Employees can access the course through www.psaccess.ca. All employees should complete this training to ensure they are fully informed of their responsibilities to protect against cyber threats in the workplace.

Does the OCIO have the right to monitor and access my computer?

Yes. The Network, its components and all Government IT assets are the property of the Employer and not the property of the Employee. Employees should be aware these assets, equipment and resources are monitored and will be searched where necessary for the maintenance or security of the Network and government's overall IT environment, or if inappropriate use is suspected, by those authorized to do so on behalf of the Employer or law enforcement agencies.

The Employer can add, remove, update and/or block any content, technical or otherwise, and view all Government records (as well as any other records which may be generated, stored on or handled by Government-issued assets), if that action is deemed necessary for the maintenance or security of the Network, or if inappropriate use is suspected. The Employer may forward IT assets and/or information to law enforcement agencies when deemed necessary.

If the OCIO is asked by a Department to provide an Employee's usage or monitoring history (e.g., list of Internet sites visited) access to an Employee's records (e.g., email, 'p' drive), the OCIO will provide this information to the Department. The OCIO will also provide access to records for the purpose of responding to an ATIPP or legal discovery request, at the request of a Department.

What are 'approved' mobile devices?

Only the OCIO can determine (i.e. approve) what mobile devices can connect to and/or be used on the Government Network. At this time, employees are not allowed to use personal mobile devices (laptops, tablets or smartphones) on the Government Network. For more information on network use of mobile devices, see the [OCIO's Mobile Devices Directive for Government Employees](#).

What type of activity is considered 'illegal or criminal'?

Please read the 'Equipment and Resources Usage Policy' in the Human Resources Policy Manual - http://www.exec.gov.nl.ca/exec/pss/working_with_us/equipment_and_resources.html.

What type of activity negatively impacts network performance?

The Government Network serves as the connection hub for all of Government's electronic systems; it is the mechanism that allows systems and Employees to communicate with each other. Some activities, however, use up a significant amount of the Government Network's resources and slow down its ability to run its systems properly. Activities that can negatively impact network performance include but are not limited to streaming video and voice (e.g., YouTube, radio stations), online gaming and the downloading large files such as movies, MP3's and other audio/video files.

If the OCIO determines that an Employee's activity is negatively impacting the performance of the Government Network, the OCIO has the authority to take steps to prevent or stop that activity.

How can I protect against SPAM, viruses and other malicious content?

As you incorporate email and the Internet into your daily work activities, you increase your exposure to Internet-based threats such as SPAM, viruses, phishing (see [FYI – Phishing Don't Get Caught](#)) and other forms of malicious content, known as 'cybercrime'. As an employee, you have a responsibility to do your part to reduce the threat of cyber-attacks. For more information on Cyber Security, visit the OCIO website at <http://www.ocio.gov.nl.ca/ocio/security/cybersecurity.html>.

To ensure cyber threats are limited, follow these steps:

1. Never disclose your government-issued username and password.
2. Never click on links or attachments in e-mails from unknown sources.
3. Never use your government-issued e-mail address for personal use.
4. Do not answer suspicious emails even if they appear legitimate.
5. Suspicious emails often appear to be from a recognized organization or client. Contact the legitimate organization or client through another means of communication (e.g., by phone; do not use the contact information in the email you received but rather from previously established contact list) and ask if they sent such an email. If uncertain, speak to your supervisor.
6. Avoid storing files locally on your government desktop or laptop. You should always store files on a network drive where they can be backed up. If you must store files temporarily on a local hard drive always ensure you are backing up the data on a regular basis. Otherwise, if your computer was compromised, you would not have a copy of your file/data and it is highly unlikely the OCIO would be able to recover any deleted/encrypted files.

What is 'licensed' software?

Licensed software, which may be free of charge or purchased, requires the user/purchaser to accept an 'end user agreement' stating conditions for using the software. For example, software purchased or obtained from the 'Apple Store' and 'Blackberry App World' is licensed. Before you acquire licensed software, OCIO cautions you to:

- Avoid use of software that requires or allows for auto-syncing with cloud services.
- Only obtain software that is needed to perform your work-related duties.
- Verify that the software is from a trusted source.
- Check that the software has a valid digital signature.
- Consult your departmental IM Director to engage the OCIO for a software review prior to purchase.

If the OCIO determines that installed licensed software is negatively impacting the security or performance of the Government Network, the OCIO has the authority to secure, update and/or remove the licensed software.

What is 'Government-approved' hardware?

Only the OCIO can determine (i.e. approve) what hardware can connect to and/or be used on the Government Network. Hardware is the physical equipment that makes up a computer system, including but not limited to laptops, desktop computers, external hard drives and peripheral devices such as monitors, printers, scanners and other multi-function devices. You are only allowed to install hardware on the Government Network that has been approved for use by the OCIO. For more information on Government-approved hardware, contact the OCIO IT Service Desk at servicedesk@gov.nl.ca or 709-729-HELP (4357).

Can I store personal photos and documents on shared drives?

No. Only Government-related files can be stored on shared drives located on the Government Network. Personal photos, music files and other personal documents cannot be stored on network drives. The Government Network is to be used for the storage of Government information only. The OCIO backs up the Network on a regular basis, which has time and cost implications for Government. The enterprise network and backup solution should only be used to house and support Government business. If you must store personal files on your government-issued computer, you should save it to your local drive (i.e. 'C' drive; My Documents, Desktop).

Does this Directive apply to personal devices?

No. At this time, employees are not allowed to use personal mobile devices (laptops, tablets or smartphones) on the Government Network. For more information on network use of mobile devices, see the [OCIO's Mobile Devices Directive for Government Employees](#). If you have been approved to use a personal device for the purpose of doing Government business prior to implementation of this Directive, you are bound by any Terms of Use document that was signed when approval to use the device was granted.

Who do I contact if I have questions about the Acceptable Use Directive?

If you have questions about the Acceptable Use Directive or this FAQ, please contact OCIOInfoProtection@gov.nl.ca.



Frequently Asked Questions (FAQs)

Information Management and Protection Policy

1. Who is responsible for the Information Management and Protection Policy?

The Office of the Chief Information Officer (OCIO) administers the Management of Information Act and is accountable to develop and implement a management program for government records in the province, provide advice to and assist public bodies with developing, implementing and maintaining record management systems and recommend policies to Treasury Board for adoption.

2. What is the purpose of the Information Management and Protection Policy?

This policy establishes the foundation for development of all Information Management and Protection policies, directives, standards, guidelines and procedures by the Office of the Chief Information Officer (OCIO) and provides the OCIO with a comprehensive approach in addressing Information Management and Protection Policy governance.

3. How was the OCIO guided in the development of the Information Management and Protection Policy?

The OCIO was guided by the relevant International Standards Organization (ISO) and Canadian General Standards Board (CGSB) standards for its policy development framework and overall approach. In addition, the development of specific policy instruments is based upon the following principles: promoting records creation, enabling transparency and legislative compliance, lifecycle management of all information in all formats, providing information authenticity, integrity and security and managing risk.

4. What responsibilities do government departments and public bodies have in relation to the Information Management and Protection Policy?

Departments and public bodies must comply with the Information Management and Protection Policy and any directives and standards released under its authority. They must develop departmental or organizational specific procedures complementary to the policies, directives, standards and guidelines established under this policy.

FREQUENTLY ASKED QUESTIONS (FAQs) – INFORMATION MANAGEMENT AND PROTECTION POLICY

5. What responsibilities do government employees or contractors have in relation to the Information Management and Protection Policy?

Government employees or contractors who create or collect information as part of their responsibility in performing work for Government must comply with the Information Management and Protection Policy. Information and records in all formats must be managed and protected throughout their lifecycle.

6. What are the Information Management and Protection Principles found within the Information Management and Protection Policy?

The development of Information Management and Protection policies, directives, standards and guidelines by the OCIO is based upon the following principles:

- i. Promoting records creation
- ii. Enabling Transparency
- iii. Enabling Legislative Compliance
- iv. Lifecycle Management of all information in all formats
- v. Providing information authenticity, integrity and security
- vi. Risk management

Supporting Materials

[Information Management and Protection Policy, TBM 2018-111](#)

Version History

Date (yyyy mm dd)	Reference
2018 07 18	Version 1.0



Frequently Asked Questions (FAQs)

Instant Messaging Directive

1. What is instant messaging?

Instant messaging is a form of real-time, direct communication between two or more parties using personal computers or other devices such as smart phones or tablets.

2. What are some examples of instant messaging technologies?

Instant messaging technologies are designed to support real-time conversational interactions. Examples of instant messaging include:

BlackBerry Messenger (BBM)

- A cross-platform messaging application available for BlackBerry, iOS devices, Android and Windows Phone platforms.

Text Messaging (Short Message Service (SMS), Multimedia Messaging Service (MMS) or iMessage)

- The text communication service component of phone, web or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices.

Skype for Business

- An instant messaging, chat, video and audio conferencing tool that allows users to communicate and collaborate with others using their computers from any location around the world

3. Why do employees use instant messaging?

Instant messages are used to facilitate the flow of business. Typically, they replace a conversation that previously occurred in person or over the phone. "On my way to the meeting," "Did you get the package?" or "Let's meet for lunch" are the types of information often exchanged via instant messaging technologies.

4. Does the OCIO back up instant messages generated or transmitted on the government network or devices?

The OCIO does not record, retain or back up instant messages. Challenges with searching and managing data stored in instant messaging logs make it difficult to segregate records that must be kept from those that should be deleted. These logs are not appropriate repositories for

FREQUENTLY ASKED QUESTIONS (FAQs) - INSTANT MESSAGING DIRECTIVE

information management purposes. It is the responsibility of the information owner to transfer instant messages to a proper government recordkeeping format where required.

5. What should I do if I need to capture the content of an instant message as a government record?

For the most part, instant messages tend to be transitory records with short-term value and do not need to be stored and managed in a records management system. Occasionally, an instant message conversation will evolve into a discussion that has business value and must be managed as a government record.

If you need to capture the content of an instant message as a government record, it is your responsibility to transfer it to an appropriate government storage system, just as you would do if it were a phone call or a verbal discussion on the way back from a meeting,

Once the conversation evolves into information that should be retained as a record the quickest way to transfer the content to an appropriate medium is to send an email to all those involved in the conversation. The process for doing this will vary depending on the technology – please see QUICK REFERENCE – Transitioning Instant Message Content to Recordkeeping Format.

6. What do I do with instant messages retained on my mobile device’s memory?

Instant messages retained on a mobile device should be regularly reviewed by the owner of the device with the following focus:

- transition instant messages that have become government records to a government recordkeeping system
- dispose of instant messages that are transitory in nature and where it has been determined that there is no business value

7. What is a government record?

A government record is a record created by or received by a public body in the conduct of its affairs and includes a Cabinet record, transitory record and an abandoned record. Disposal or destruction of a government record must be approved by the Government Records Committee (GRC).

If an instant message is determined to be a government record it must be managed appropriately by transferring it to an approved government recordkeeping system. It is the content of a message not its format which determines whether it is a government record.

8. What is a transitory record?

A transitory record is a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can and should be securely destroyed when no longer of value. Destruction of transitory records does not require authorization of the GRC. It is not necessary to retain instant message that have been determined to be transitory.

FREQUENTLY ASKED QUESTIONS (FAQs) - INSTANT MESSAGING DIRECTIVE

Supporting Materials

DIRECTIVE – Instant Messaging

https://www.ocio.gov.nl.ca/ocio/instant_messaging_directive.pdf

FYI – Instant Messaging Directive

https://www.ocio.gov.nl.ca/ocio/instant_messaging_fyi.pdf

QUICK REFERENCE – Transitioning Instant Message Content to Recordkeeping Format

https://www.ocio.gov.nl.ca/ocio/instant_messaging_quickreference.pdf

FYI – Identifying and Disposing of Transitory Records

<https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/transitoryrecords.pdf>

Version History

Date (yyyy mm dd)	Reference
2012 02 01	Version 1.0
2018 09 24	Version 2.0

Frequently Asked Questions

1. Why can't I use a non-government email account for work purposes?

Government employees are issued an email account to conduct work on behalf of a public body. These email accounts are managed by the Office of the Chief Information Officer and proper security precautions are applied.

Records created as part of normal business of a public body must be captured in an official government storage area such as network drive and paper file. This ensures that government record keeping systems are efficient and effective and that files are accessible in the event of operational requirements, access to information requests, litigation, etc.

2. What do I do if I have to use my personal account for government business?

- If an individual must use a personal or non-government email account to transmit a government record, they need to ensure that the record is saved to an appropriate government storage location (e.g. government email account, network drive, paper file, etc.). This returns the record to the proper custody and control of the public body and providing accessibility of the record.
- Once saved to an appropriate government storage location, the initial email should be immediately deleted from the individual's personal or non-government email account.
- Personal or confidential information emailed to a personal or non-government account should be limited to the least amount necessary to deal with the exceptional circumstance. Email outside of the government network may not be secure while in transit and the use of encryption is recommended. Please consult with Information Management staff in your department for advice on encryption tools.
- If a legitimate ongoing business need to use a non-government email account is identified, the public body must consult with the OCIO on the procurement of the account/service to ensure appropriate security requirements are met.

3. What are some examples of non-government email accounts?

Examples of non-government email accounts include:

- janedoe@yahoo.com, janedoe@hotmail.com, janedoe@gmail.com, etc.

4. What is a government record?

A government record is a record created by or received by an individual on behalf of a public body in the conduct of its affairs.

5. Are emails sent to my personal/non-government account government records?

Yes, they can be if they involve information about the business function of government.

An email sent through a private email account used to do government business falls under the province's *Access to Information and Protection of Privacy* laws, and measures should be taken to store the email in an appropriate government storage location. It is the responsibility of the employee to forward/transfer the personal email to a government storage area for long term accessibility.

6. What should I do if I suspect the content of an email sent to a personal/non-government email account should be captured as an official government record?

If you feel that the content of an email sent to a personal/non-government account should be retained as a government record, it is your responsibility to transfer/forward the email to an official government storage area. This will ensure the record is available for future reference in your department.

Once transferred to an appropriate government location, the original email should be deleted from the personal/non-government account immediately.

It is recommended the employee who received the email to their personal/non-government account respond to the sender and advise that all inquiries relating to work on behalf of a public body should be sent to an official government email account (indicate specific email address if appropriate).

7. Will consultants hired to complete work on behalf of the province require a government email account?

A consultant does not require a government email account provided that all government records relevant to a project are transferred/forwarded to an official government storage area. It is recommended that an individual in the public body accept the responsibility for capturing the records.

Processes should be developed to confirm proper records transfer, retention and documentation practices are followed. This will ensure the public body is meeting its legislative compliance requirements.

An exception to use a personal/non-government account for work in support of government should be specifically approved by the head of the public body.

8. When am I permitted to use my personal or non-government email account?

Individuals may only forward email from their government-issued account to a non-government email account under either of the following conditions:

- Use of the non-government account for government work purposes has been specifically approved by the head of the public body or approved designate to whom the individual reports.

- Government email is inaccessible; email should be transferred to an appropriate government storage location as soon as possible.
- Government approved IT asset assigned is malfunctioning (i.e. blackberry, laptop, tablet)
- Content is already publicly available.
- Email is of a personal nature that is either not work related or pertains to the individual's relationship with the public body as an employer.

Note: If personal or confidential information is emailed using a personal or non-government account it should be encrypted and should be limited to the least amount necessary to deal with the exceptional circumstance.

Frequently Asked Questions – Corporate Records and Information Management Standard (C-RIMS)

What is C-RIMS?

The Corporate Records and Information Management (C-RIMS) is a standard classification plan and records retention and disposal schedule used for the management of corporate records of the Government of Newfoundland and Labrador. Corporate records, often referred to as administrative records, are those created by all organizations to support administrative functions, including human resources, general administration, facilities management, financial management, information and information technology management, and equipment and supplies (material) management. Because the value of these records is consistent across Government Departments, C-RIMS has been developed by the Office of the Chief Information Officer (OCIO) as a standard for their management. C-RIMS replaces the Information Management System for Administrative Records (IMSAR).

What is the difference between C-RIMS and IMSAR?

IMSAR (Information Management System for Administrative Records) was initially released in 1999 as an integrated records classification system and retention and disposal schedule for administrative records of the Government of Newfoundland and Labrador. After ten years of use, IMSAR needed to be updated to reflect changes in the Government's approach to information management. C-RIMS updates terminology and, where appropriate, retention and disposition, for common records found throughout Government. C-RIMS also captures changes in role and mandate of various departments.

One of the most obvious differences is the use of the term "corporate records" to replace "administrative records"; prompting the change in the title of the standard.

Created by the Information Management Branch (IMB) of the Office of the Chief Information Officer (OCIO) in conjunction with The Rooms Provincial Archives and the Information Management Standards Board (IMSB), C-RIMS is a key component of any departmental information management program.

Is C-RIMS replacing IMSAR?

Yes. IMSAR will lapse in May 2010. During this year, departments currently using IMSAR may seek assistance from OCIO and the GRC as required to their transition to C-RIMS. It is anticipated that by May 2010 departments currently using IMSAR will have transitioned to C-RIMS.

What do I do if my department is already using IMSAR?

Departments and public bodies that currently use IMSAR will be notified to signify their intent to replace IMSAR with C-RIMS. Assistance will be provided by OCIO as required to enable the transition from IMSAR to C-RIMS.

Can I use IMSAR instead of C-RIMS?

No. IMSAR is now replaced by C-RIMS. There will be no new approvals of IMSAR. The Government Records Committee will not accept transfers or disposal notification with references and/or codes from IMSAR. Departments currently using IMSAR are strongly encouraged to develop a plan to transition to C-RIMS. Departments that have not implemented IMSAR are expected to implement C-RIMS for the management of records covered by C-RIMS.

How does my department get started using C-RIMS?

Departments and public bodies will write to the Government Records Committee signifying their intent to implement C-RIMS. Their request will be accompanied by a properly completed and signed C-RIMS Form. This form is available on the OCIO website. Monitoring of C-RIMS implementation will be done by the Government Records Lifecycle Management Unit of the OCIO and will be a condition of C-RIMS approval. Regular reporting to the Government Records Committee will also be required, on a schedule to be determined.

Will training be provided on how to use C-RIMS?

C-RIMS was designed to be easy to interpret with detailed explanations of the structure and content included in the introductory sections. There will be no formal training component provided. Advice and guidance on the use of C-RIMS or the interpretation of records series will be provided by the Government Records Lifecycle Management Unit of the OCIO as required.

Can a Crown Corporation use C-RIMS

Crown corporations may apply the classification structure and descriptions of record series found in C-RIMS as these are common across all organizations. However each corporation is advised to verify with their internal resources including information management, legal counsel, finance and audit representatives that the proposed records retention periods and dispositions are appropriate.



Records Retention and Disposal Schedules (RRDS) Frequently Asked Questions

[What is a Records Retention and Disposal Schedule \(RRDS\)?](#)

[Why Develop and Implement Records Retention and Disposal Schedule \(RRDS\)?](#)

[What are the Roles and Responsibilities Related to Records Retention and Disposal Schedules \(RRDS\)?](#)

[How do I make changes to an already approved Records Retention and Disposal Schedule \(RRDS\)?](#)

[How do I transfer ownership of an existing Records Retention and Disposal Schedule \(RRDS\) to another department?](#)

[Do I have to use the Records Retention and Disposal Schedule Standard?](#)

What is a Records Retention and Disposal Schedule (RRDS)?

The records retention and disposal schedule (RRDS or schedule) prescribes records retention periods and disposal plans, can apply to records in any format and authorizes disposal of records in a legal manner. The RRDS can be for all records in an organization, or for the records of a specific branch or division. It can encompass all types of records within an organization, or may be limited to specific types or record series as they are sometimes called.

The RRDS (schedule) should include, at a minimum:

- Descriptions of the records covered by the schedule sufficient to allow users to understand which records are included.
- The retention periods of the records in all stages of their lifecycle: from active, through semi-active, to final disposal.
- Legally approved disposal for the records in the schedule – under the [Management of Information Act](#) and the [Rooms Act](#), legal disposal means one of two things: either records are destroyed or they are transferred to The Rooms Provincial Archives for permanent preservation.
- Identification of Vital Records. These are records which are required to resume business of the organization in the event of catastrophe (e.g., Cabinet records, the documents describing the operations of essential IT systems, and the organization's main financial systems).
- The identity of the Office of Primary Responsibility (OPR). The OPR is the department or public body; or the division or section of a department or public body that created the record in the course of its mandate and that will be responsible for implementing and maintaining the schedule.

Why Develop and Implement Records Retention and Disposal Schedules (RRDS)?

The [Management of Information Act](#) requires a request be submitted to the [Government Records Committee \(GRC\)](#) to dispose of government records. The Records Retention and Disposal Schedule (RRDS) is the recommended tool used for the legal disposal of government records, once approved the RRDS can be used on an ongoing basis to manage records.



Failure to implement RRDS as a regular part of ongoing operations may result in:

- Delay in provision of services as employees are forced to search through outdated or semi-active records to respond to inquiries.
- Inefficient use of resources including:
 - Budget unnecessarily spent on physical or electronic storage space.
 - Cost to continue backup and recovery of electronic information which is no longer required.
 - Time and resources wasted on inefficient search and retrieval.
- Embarrassment and/or legal implications if information is disposed of without appropriate authorization.

What are the Roles and Responsibilities Related to Records Retention and Disposal Schedules (RRDS)?

A Records Retention and Disposal Schedule (RRDS) is an important legal document. Multiple stakeholders are involved in the development and implementation of RRDS including:

Departments and Public Bodies

- Commit to use of the [Corporate Records and Information Management Standard \(C-RIMS\)](#).
- [Develop RRDS for Operational Records](#).
- Submit RRDS to the [Government Records Committee](#).
- Negotiate terms of transfer of archival records to The Rooms Provincial Archives.
- Implement RRDS as a part of ongoing operations.
- Perform periodic review of RRDS to identify if changes are required.
- Update or develop new RRDS as required in the event of change in mandate, organizational change, new lines of business, etc..

Office of the Chief Information Officer (OCIO) - Information Management Advisory Services Branch

- Define and publish directives, standards and guidelines.
- Provide advice on government records lifecycle management.
- Manage a semi-active records storage program for government.
- Manage the approval process for RRDS.
- Support the operations of the [Government Records Committee](#) and manage the [Provincial Records Centre](#).

The Rooms Provincial Archives

- Preserve archival government records as mandated by the [Rooms Act](#).
- Review schedules to identify records of enduring value (Archival Appraisal).
- Negotiate terms of transfer of archival records to The Rooms Provincial Archives.
- Research and describe records including Administrative Histories.
- Research access provisions to records according to ATIPP exceptions and exemptions.
- Conserve records as required, including reformatting.



Government Records Committee (GRC)

- Establish and revise schedules for the retention, disposal, destruction or transfer of records.
- Make recommendations to the Minister respecting government records to be forwarded to [The Rooms Provincial Archives](#).
- Establish disposal and destruction standards and guidelines for the lawful disposal and destruction of government records.
- Make recommendations to the Minister regarding the removal, disposal and destruction of records.

How do I make changes to an already approved Records Retention and Disposal Schedule (RRDS)?

Updates to the RRDS can either require an amendment to an existing schedule or depending on the level of changes required a new one be created, superseding the old. In any event, it must be approved by the GRC.

Amendments are minor revisions to the schedule that does not alter the context of the schedule. Amendments include, but are not limited to:

- Increases or decreases in the overall retention period.
- Changes to final disposition.
- Minor changes to Record Series Title or Description.
- Minor changes to Program/Service Name or Functions.
- Changes to ATIPP Exceptions.
- Changes in ownership in its entirety.
- Changes in official media type.

Schedules that require major revisions which alters the context of the schedule must be submitted as a new RRDS, voiding the old. Major changes include, but are not limited to:

- Addition or deletion of a Record Series.
- Addition or deletion of a Program/ Service or Function.

If a schedule is no longer required because the program or function is no longer a mandate of Government, the originating department must submit a memo to the GRC indicating that the previously approved retention schedule is now void and can no longer be applied.

How do I transfer ownership of an existing Records Retention and Disposal Schedule (RRDS) to another department?

Transferring the ownership of government records is required when there is an administrative change within Government and the mandate still exists for a records series.

The originating department is responsible for notifying the Government Records Committee (GRC) that a transfer of ownership is imminent or has already taken place. This provides authorization to the [Office of Primary Responsibility](#) to continue implementation of approved schedules. Departments must ensure that



all legacy records reflect the transfer of ownership including, but not limited to: RRDS, C-RIMS Implementation Agreements and Semi-Active records stored offsite.

The following template must be used when notifying the GRC of a transfer of ownership.

- [Template Memorandum for Transferring Ownership](#)

Do I have to use the Records Retention and Disposal Schedule (RRDS) Standard Template?

Yes. OCIO standards are mandatory for users to follow and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. Standards are usually defined to support the policies and directives and are supported by Guidelines, where applicable. OCIO Standards derive from **Information Management and Protection Policy, TBM 2009-335** approved by Treasury Board on November 19, 2009.



Records Retention and Disposal Schedules (RRDS) Frequently Asked Questions

[What is a Records Retention and Disposal Schedule \(RRDS\)?](#)

[Why Develop and Implement Records Retention and Disposal Schedule \(RRDS\)?](#)

[What are the Roles and Responsibilities Related to Records Retention and Disposal Schedules \(RRDS\)?](#)

[How do I make changes to an already approved Records Retention and Disposal Schedule \(RRDS\)?](#)

[How do I transfer ownership of an existing Records Retention and Disposal Schedule \(RRDS\) to another department?](#)

[Do I have to use the Records Retention and Disposal Schedule Standard?](#)

What is a Records Retention and Disposal Schedule (RRDS)?

The records retention and disposal schedule (RRDS or schedule) prescribes records retention periods and disposal plans, can apply to records in any format and authorizes disposal of records in a legal manner. The RRDS can be for all records in an organization, or for the records of a specific branch or division. It can encompass all types of records within an organization, or may be limited to specific types or record series as they are sometimes called.

The RRDS (schedule) should include, at a minimum:

- Descriptions of the records covered by the schedule sufficient to allow users to understand which records are included.
- The retention periods of the records in all stages of their lifecycle: from active, through semi-active, to final disposal.
- Legally approved disposal for the records in the schedule – under the [Management of Information Act](#) and the [Rooms Act](#), legal disposal means one of two things: either records are destroyed or they are transferred to The Rooms Provincial Archives for permanent preservation.
- Identification of Vital Records. These are records which are required to resume business of the organization in the event of catastrophe (e.g., Cabinet records, the documents describing the operations of essential IT systems, and the organization's main financial systems).
- The identity of the Office of Primary Responsibility (OPR). The OPR is the department or public body; or the division or section of a department or public body that created the record in the course of its mandate and that will be responsible for implementing and maintaining the schedule.

Why Develop and Implement Records Retention and Disposal Schedules (RRDS)?

The [Management of Information Act](#) requires a request be submitted to the [Government Records Committee \(GRC\)](#) to dispose of government records. The Records Retention and Disposal Schedule (RRDS) is the recommended tool used for the legal disposal of government records, once approved the RRDS can be used on an ongoing basis to manage records.



Failure to implement RRDS as a regular part of ongoing operations may result in:

- Delay in provision of services as employees are forced to search through outdated or semi-active records to respond to inquiries.
- Inefficient use of resources including:
 - Budget unnecessarily spent on physical or electronic storage space.
 - Cost to continue backup and recovery of electronic information which is no longer required.
 - Time and resources wasted on inefficient search and retrieval.
- Embarrassment and/or legal implications if information is disposed of without appropriate authorization.

What are the Roles and Responsibilities Related to Records Retention and Disposal Schedules (RRDS)?

A Records Retention and Disposal Schedule (RRDS) is an important legal document. Multiple stakeholders are involved in the development and implementation of RRDS including:

Departments and Public Bodies

- Commit to use of the [Corporate Records and Information Management Standard \(C-RIMS\)](#).
- [Develop RRDS for Operational Records](#).
- Submit RRDS to the [Government Records Committee](#).
- Negotiate terms of transfer of archival records to The Rooms Provincial Archives.
- Implement RRDS as a part of ongoing operations.
- Perform periodic review of RRDS to identify if changes are required.
- Update or develop new RRDS as required in the event of change in mandate, organizational change, new lines of business, etc..

Office of the Chief Information Officer (OCIO) - Information Management Advisory Services Branch

- Define and publish directives, standards and guidelines.
- Provide advice on government records lifecycle management.
- Manage a semi-active records storage program for government.
- Manage the approval process for RRDS.
- Support the operations of the [Government Records Committee](#) and manage the [Provincial Records Centre](#).

The Rooms Provincial Archives

- Preserve archival government records as mandated by the [Rooms Act](#).
- Review schedules to identify records of enduring value (Archival Appraisal).
- Negotiate terms of transfer of archival records to The Rooms Provincial Archives.
- Research and describe records including Administrative Histories.
- Research access provisions to records according to ATIPP exceptions and exemptions.
- Conserve records as required, including reformatting.



Government Records Committee (GRC)

- Establish and revise schedules for the retention, disposal, destruction or transfer of records.
- Make recommendations to the Minister respecting government records to be forwarded to [The Rooms Provincial Archives](#).
- Establish disposal and destruction standards and guidelines for the lawful disposal and destruction of government records.
- Make recommendations to the Minister regarding the removal, disposal and destruction of records.

How do I make changes to an already approved Records Retention and Disposal Schedule (RRDS)?

Updates to the RRDS can either require an amendment to an existing schedule or depending on the level of changes required a new one be created, superseding the old. In any event, it must be approved by the GRC.

Amendments are minor revisions to the schedule that does not alter the context of the schedule. Amendments include, but are not limited to:

- Increases or decreases in the overall retention period.
- Changes to final disposition.
- Minor changes to Record Series Title or Description.
- Minor changes to Program/Service Name or Functions.
- Changes to ATIPP Exceptions.
- Changes in ownership in its entirety.
- Changes in official media type.

Schedules that require major revisions which alters the context of the schedule must be submitted as a new RRDS, voiding the old. Major changes include, but are not limited to:

- Addition or deletion of a Record Series.
- Addition or deletion of a Program/ Service or Function.

If a schedule is no longer required because the program or function is no longer a mandate of Government, the originating department must submit a memo to the GRC indicating that the previously approved retention schedule is now void and can no longer be applied.

How do I transfer ownership of an existing Records Retention and Disposal Schedule (RRDS) to another department?

Transferring the ownership of government records is required when there is an administrative change within Government and the mandate still exists for a records series.

The originating department is responsible for notifying the Government Records Committee (GRC) that a transfer of ownership is imminent or has already taken place. This provides authorization to the [Office of Primary Responsibility](#) to continue implementation of approved schedules. Departments must ensure that



all legacy records reflect the transfer of ownership including, but not limited to: RRDS, C-RIMS Implementation Agreements and Semi-Active records stored offsite.

The following template must be used when notifying the GRC of a transfer of ownership.

- [Template Memorandum for Transferring Ownership](#)

Do I have to use the Records Retention and Disposal Schedule (RRDS) Standard Template?

Yes. OCIO standards are mandatory for users to follow and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. Standards are usually defined to support the policies and directives and are supported by Guidelines, where applicable. OCIO Standards derive from **Information Management and Protection Policy, TBM 2009-335** approved by Treasury Board on November 19, 2009.



One Time Disposal Frequently Asked Questions

[What is a One Time Disposal?](#)

[Why use a One Time Disposal Submission?](#)

[Do I have to follow the One Time Disposal Standard?](#)

What is a One Time Disposal?

An OTD Submission is used to dispose of a backlog of inactive records not covered under a [retention schedule](#). One Time Disposal (OTD) applies to records in any format and authorizes disposal of records in a legal manner. The OTD can be for records of a specific branch or division. It can encompass all types of records within an organization, or may be limited to specific record types or record series as they are sometimes called.

The [Management of Information Act](#) mandates the [Government Records Committee \(GRC\)](#) to make recommendations to the Minister relating to the disposal of government records. The One Time Disposal Submission is one of the recommended tools used for the legal disposal of government records.

Why Use a One Time Disposal Submission?

A One Time Disposal (OTD) Submission is an alternative to the use of a records retention and disposal schedule to dispose of a backlog of inactive records. This option may be used when records are the result of an activity no longer in progress (e.g. organizational unit, service or function that no longer exists) or where the value of the records supports a high-level decision on their disposal (e.g. administrative records that are 7+ years old).

The process includes an inventory of the records and the submission of an OTD Submission form to the Government Records Committee.

Do I have to follow the One Time Disposal Standard Template?

Yes. OCIO standards are mandatory for users to follow and dictate uniform ways of operating. Standards provide tactical blueprints for implementation of policies and directives. Standards are usually defined to support the policies and directives and are supported by Guidelines, where applicable. OCIO Standards derive from Information Management and Protection Policy, **TBM 2009-335** approved by Treasury Board on November 19, 2009.



Government Records Committee (GRC) Frequently Asked Questions

[What is the Government Records Committee \(GRC\)?](#)

[Who sits on the GRC?](#)

[How do I know if I fall under the purview of the Government Records Committee?](#)

[Do I need GRC approval to dispose of government records?](#)

[How do I get approval to dispose of government records?](#)

[When does the committee meet?](#)

[What is the deadline for submissions to the monthly meeting of the Government Records Committee?](#)

[What happens if I miss the deadline?](#)

[Who do I direct submissions to?](#)

What is the Government Records Committee (GRC)?

The Government Records Committee is established by the *Management of Information Act*. The GRC establishes and revises schedules for the retention, disposal, destruction or transfer of records; makes recommendations to the minister respecting government records to be forwarded to the archives; establishes disposal and destruction standards and guidelines for the lawful disposal and destruction of government records; and makes recommendations to the minister regarding the removal, disposal and destruction of records.

Who sits on the GRC?

The Government Records Committee consists of the following members:

- 1) Director of The Rooms Provincial Archives;
- 2) Deputy Minister of Justice or designate;
- 3) Deputy Minister of Finance or designate;
- 4) Chief Information Officer or designate;
- 5) Other persons whom the minister, appointed under the *Executive Council Act*, may appoint.

The Chief Information Officer or designate is the chair of the GRC with the OCIO providing administrative support.

How do I know if I fall under the purview of the Government Records Committee?

Public bodies as defined by the Management of Information Act, fall under the purview of the Government Records Committee.



Public bodies are defined as:

- i. a department created under the Executive Council Act or a branch of the executive government of the province,
- ii. a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown,
- iii. a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a minister of the Crown,
- iv. a court established under an Act of the province, and the House of Assembly and committees of the House of Assembly.

Do I need GRC approval to dispose of government records?

With the exception of transitory records or copies of convenience, the approval of the GRC is required to dispose of government records.

How do I get approval to dispose of government records?

Approval is granted by the GRC to dispose of records using one of two standards: Records Retention and Disposal Schedules (RRDS) or One Time Disposal Submissions (OTD). These standards, along with instructions for use may be found at:

<http://www.ocio.gov.nl.ca/ocio/im/disposal.html>

When does the committee meet?

Meetings are scheduled for the second Tuesday of the month. The committee does not meet in July and August.

What is the deadline for submissions to the monthly meeting of the Government Records Committee?

In order to be considered at the meeting submissions must be in by the first Tuesday of the month – 1 week prior to the meeting.

What happens if I miss the deadline?

The department will be notified that they did not meet the deadline and that the submission will go forward at the next scheduled GRC meeting.



Who do I direct submissions to?

Submissions must be forwarded electronically to the [Government Records Lifecycle Management \(GRLM\)](#) unit and the [Government Records Archivist](#) for review and appraisal prior to the department obtaining required signatures.

Once reviewed the department must obtain required signatures and forward signed originals to the following address:

Government Records Committee

Office of the Chief Information Officer
Provincial Records Centre
P.O. Box 8700
190 East White Hills Road
Building 1050, Pleasantville
St. John's, NL A1B 4J6
Telephone: 1-709-729-3628
E-mail: GRLM@Gov.NL.Ca

Provincial Records Centre FAQs

1. [What is the Provincial Records Centre \(PRC\) and what services do they offer?](#)
2. [What are the hours of operation?](#)
3. [How do I contact the Provincial Records Centre \(PRC\)?](#)
4. [What records are eligible for storage at the Provincial Records Centre \(PRC\)?](#)
5. [What are the options if the records do not meet the criteria for storage at the PRC?](#)
6. [How can I find out if my department has records stored at the Provincial Records Centre \(PRC\)?](#)
7. [What is the process for transferring records to the Provincial Records Centre \(PRC\)?](#)
8. [Who is responsible for arranging courier services and associated costs with delivery and pick-up of records \(i.e. courier costs\)?](#)
9. [How should I prepare records for offsite storage?](#)
10. [Does it matter what kind of box I use for the records?](#)
11. [Can I fill out one transfer form for multiple boxes?](#)
12. [How will I know when my boxes are delivered to the PRC?](#)
13. [Do I need special permission to request information on behalf of my department?](#)
14. [How do I request a file or box from offsite storage?](#)
15. [Can I sign out multiple boxes using the same form?](#)
16. [How is a file delivered to the department when requested?](#)
17. [How long does it take to get a file or box from offsite storage?](#)
18. [How long can I keep a file or box?](#)
19. [How do I return a file?](#)
20. [Can I view boxes onsite?](#)
21. [Who do I notify if records stored at the PRC need to be placed on legal hold or that a legal hold currently in place is lifted?](#)

1. **What is the Provincial Records Centre (PRC) and what services do they offer?**

The Provincial Records Centre (PRC) is a safe, secure storage facility for semi-active government records.

Services include, but are not limited to:

- Storage of government records.
- Access to records in storage and facilitates the delivery and pick-up of records upon request.
- Administrative support to the Government Records Committee (GRC).
- Facilitates the onsite disposal of records stored at the PRC that have been approved for destruction by the GRC.

2. **What are the hours of operation?**

The Provincial Records Centre (PRC) is open Monday to Friday from 8:00 am to 4:00 pm and closed during the lunch hour between 12:30 and 1:30 pm.

Summer hours are Monday to Friday from 8:00 am to 3:30 pm and closed during the lunch hour between 12:30 and 1:30 pm.

3. How do I contact the Provincial Records Centre (PRC)?

Provincial Records Centre (Building 1050)
P.O Box 8700
190 East White Hills Rd, Pleasantville
St. John's, NL A1B 4J6
Telephone: 1-709-729-3628
Email: grlm@gov.nl.ca

4. What records are eligible for storage at the Provincial Records Centre (PRC)?

The PRC provides secure storage for the following classes of semi-active government records:

- Vital Records that are identified as either indispensable to a mission critical business operation or essential for the continuation of an organization during or following a disaster.
- Records for which the legal or operational needs of the department dictate that custody and/or control of the information must remain within government.
- Records which, due to their enduring value or historical significance, are to be transferred to The Rooms Provincial Archives Division when no longer required by the department or public body.
- Records which have longer than usual semi-active retention periods may be considered, to lessen the burden of storage costs on departments and public bodies.
- Records must have an approved Records Retention and Disposal Schedule

5. What are the options if the records do not meet the criteria for storage at the PRC?

There is a standing offer in place for commercial records storage with Iron Mountain. Contact your Finance Division or GPA for a copy.

6. How can I find out if my department has records stored at the Provincial Records Centre (PRC)?

Departments can request a copy of their Departmental Information Holdings by emailing the Provincial Records Centre (PRC).

7. What is the process for transferring records to the Provincial Records Centre (PRC)?

Consultation with PRC staff is required prior to any physical transfer of records to the facility. Departments and public bodies must fully complete and electronically submit the Records Transfer Form to the PRC for their review and approval.

Once all forms have been reviewed and approved by PRC staff, departments and public

bodies will be contacted to determine a suitable delivery date and provide further instruction.

8. Who is responsible for arranging courier services and associated costs with delivery and pick-up of records (i.e. courier costs)?

In consultation with the Provincial Records Centre (PRC), the requesting department is responsible for making all arrangements with the courier company for pick-up and delivery services.

It is also the responsibility of the requesting department to pay all associated costs.

9. How should I prepare records for offsite storage?

Departments and public bodies should transfer records in a safe and secure manner. Things to consider include, but not limited to:

- Ensuring box has no other markings on it other than a unique identifier.
- Ensuring boxes are secured with tape or some other form of "tamper proof" mechanism.
- Using a bonded courier or delivery vehicle that doesn't expose the records to outside elements or theft (i.e enclosed vehicle instead of an open pick-up truck).

Refer to IM Advisory for Preparing Paper Records for Offsite Storage.

10. Does it matter what kind of box I use for the records?

Yes. The Provincial Records Centre (PRC) only accepts one cubic foot cardboard storage boxes to conform to the size of your shelving units. It is preferred that the boxes have handles and attached lids as it allows for easy and safe retrievals.

There is a standing offer in place for storage boxes. Contact your Finance Division or GPA for a copy.

11. Can I fill out one transfer form for multiple boxes?

No. A records transfer sheet must be completed for each box of records being transferred to the Provincial Records Centre (PRC) as it contains a file listing specific to the box.

A copy of the transfer and file listing must be included in each box upon transfer.

12. How will I know when my boxes are delivered to the PRC?

You will receive confirmation by email that the transfer was received and the details surrounding it.

13. Do I need special permission to request information on behalf of my department?

Yes. Individuals requesting information on behalf of their department must be authorized and listed on a PRC Client Chart of Authority for their department. Permission would normally be given through a departmental IM director or an authorized person can request the file on your behalf.

14. How do I request a file or box from offsite storage?

The authorized requestor must complete a Request for Records Form and send it electronically to grlm@gov.nl.ca.

15. Can I sign out multiple boxes using the same form?

Yes. You can sign out multiple boxes using the same form if they are being delivered to the same location.

16. How is a file delivered to the department when requested?

All internal mail within the St. John's area will be delivered by Transportation and Works (TW) Mail Services Division, unless otherwise specified. All internal mail outside of the St. John's area will be sent by Xpresspost and should be received within 3-5 business days.

The Government Purchasing Agency (GPA) maintains Master Standing Offer Agreements (MSOA) with courier companies for the secure transport of materials. Contact your departments' financial operations officer to access the most updated MSOAs.

17. How long does it take to get a file or box from offsite storage?

The request will be ready for pick-up within 24 hours of receipt, unless otherwise notified. The delivery time will depend on the method of delivery used.

Internal Mail Services:

Departments or public bodies serviced by internal mail will generally take 1 to 2 business days. Departments or public bodies serviced by Xpresspost will generally take 3 to 5 business days.

Courier Services:

PRC staff will notify requester via email the size and weight of records so that they may arrange pickup. Regular service will be picked up within 2 hours and rush service will be picked up within 1 hour of notification.

18. How long can I keep a file or box?

Temporary loans must be returned within 30 days. It is the responsibility of the requester

to notify the PRC in the event that records are required for a longer period of time.

Departments can also do a permanent withdrawal by selecting that option on the Request for Records Form.

19. How do I return a file?

Send the file in a secure envelope or package to the Provincial Records Centre, Building 1050, 190 East White Hills Road, St. John's, NL A1A 5J7

20. Can I view boxes onsite?

Yes. Contact the Provincial Records Centre (PRC) to arrange a viewing time.

21. Who do I notify if records stored at the PRC need to be placed on legal hold or that a legal hold currently in place is lifted?

Send an email to the Provincial Records Centre (PRC) stating that records are on legal hold. Ensure you provide a listing of boxes that are placed on legal hold and any necessary access restrictions.

When the legal hold is lifted departments must notify the PRC immediately.



9. Quick Reference

- 9.1. Transferring Records to The Rooms Provincial Archives Division
- 9.2. Summary of ATIPP Exceptions
- 9.3. Records Retention and Disposal Schedule Amendments
- 9.4. Transitioning Instant Message Content to Recordkeeping Format

The Rooms Provincial Archives Division

Transferring Records To The Rooms Provincial Archives

Overview

The Rooms Provincial Archives division is mandated, through the Rooms Act, to preserve those records of the Government of Newfoundland and Labrador which are deemed to have legal, fiscal, evidential or research value. The Rooms Provincial Archives will accept records that have been pre-approved by the Government Records Committee (GRC) and having the disposition of Archive or Selective Retention on the Records Retention and Disposal Schedule (RRDS).

For further information on transferring records to The Rooms Provincial Archives, contact the Government Records Archivist at jmowbray@therooms.ca.

General Advice

- Records will be those that have a disposition of archive or selective retention rather than destroy.
- Apply selective retention criteria to records described in schedule.
- Remove transitory records from the series including surplus copies, non-annotated versions, non-file items and drafts or working papers. There are some exceptions to drafts being non-archival and this will be determined according to the public body that is the creator, and the type of record.
- Records that are in electronic format need to be printed prior to transfer.
- Boxes must contain a single records series.
- Each box must include a detailed file listing.
- Copies of transfer lists must be retained by the department or public body. If records are required the RRDS number, the box number and file title must be provided. Please note: file review must be completed in The Rooms Provincial Archives reference room – unless there are exceptional circumstances.
- Access to Information and Protection of Privacy Act (ATIPPA) issues ie: exceptions to access for **each file** must be identified. If there is access protocol this should be also documented in the RRDS and transfer records. Due to some ATIPPA exceptions to access, - the creating department will be responsible to determine access for some records transferred to the Rooms Provincial Archives.



Summary of Access to Information and Protection of Privacy (ATIPP)

Exceptions

27. Cabinet confidences 2

28. Local public body confidences..... 3

29. Policy advice or recommendations 3

30. Legal advice 5

31. Disclosure harmful to law enforcement..... 5

32. Confidential evaluations 7

33. Information from a workplace investigation 7

34. Disclosure harmful to intergovernmental relations or negotiations 8

35. Disclosure harmful to the financial or economic interests of a public body 9

36. Disclosure harmful to conservation 10

37. Disclosure harmful to individual or public safety 10

38. Disclosure harmful to labour relations interests of public body as employer 10

39. Disclosure harmful to business interests of a third party 11

40. Disclosure harmful to personal privacy 12

41. Disclosure of House of Assembly service and statutory office records..... 15



27. Cabinet confidences

27. (1) In this section, "cabinet record" means
- (a) advice, recommendations or policy considerations submitted or prepared for submission to the Cabinet;
 - (b) draft legislation or regulations submitted or prepared for submission to the Cabinet;
 - (c) a memorandum, the purpose of which is to present proposals or recommendations to the Cabinet;
 - (d) a discussion paper, policy analysis, proposal, advice or briefing material prepared for Cabinet, excluding the sections of these records that are factual or background material;
 - (e) an agenda, minute or other record of Cabinet recording deliberations or decisions of the Cabinet;
 - (f) a record used for or which reflects communications or discussions among ministers on matters relating to the making of government decisions or the formulation of government policy;
 - (g) a record created for or by a minister for the purpose of briefing that minister on a matter for the Cabinet;
 - (h) a record created during the process of developing or preparing a submission for the Cabinet; and
 - (i) that portion of a record which contains information about the contents of a record within a class of information referred to in paragraphs (a) to (h).
- (2) The head of a public body shall refuse to disclose to an applicant
- (a) a cabinet record; or
 - (b) information in a record other than a cabinet record that would reveal the substance of deliberations of Cabinet.
- (3) Notwithstanding subsection (2), the Clerk of the Executive Council may disclose a cabinet record or information that would reveal the substance of deliberations of Cabinet where the Clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.



- (4) Subsections (1) and (2) do not apply to
- (a) information in a record that has been in existence for 20 years or more; or
- (b) information in a record of a decision made by the Cabinet on an appeal under an Act.

28. Local public body confidences

28. (1) The head of a local public body may refuse to disclose to an applicant information that would reveal

- (a) a draft of a resolution, by-law or other legal instrument by which the local public body acts;
- (b) a draft of a private Bill; or
- (c) the substance of deliberations of a meeting of its elected officials or governing body or a committee of its elected officials or governing body, where an Act authorizes the holding of a meeting in the absence of the public.

(2) Subsection (1) does not apply where

- (a) the draft of a resolution, by-law or other legal instrument, a private Bill or the subject matter of deliberations has been considered, other than incidentally, in a meeting open to the public; or
- (b) the information referred to in subsection (1) is in a record that has been in existence for 15 years or more.

29. Policy advice or recommendations

29. (1) The head of a public body may refuse to disclose to an applicant information that would reveal

- (a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or minister;
- (b) the contents of a formal research report or audit report that in the opinion of the head of the public body is incomplete and in respect of which a request or order for completion has been made by the head within 65 business days of delivery of the report; or



- (c) draft legislation or regulations.
- (2) The head of a public body shall not refuse to disclose under subsection (1)
 - (a) factual material;
 - (b) a public opinion poll;
 - (c) a statistical survey;
 - (d) an appraisal;
 - (e) an environmental impact statement or similar information;
 - (f) a final report or final audit on the performance or efficiency of a public body or on any of its programs or policies;
 - (g) a consumer test report or a report of a test carried out on a product to test equipment of the public body;
 - (h) a feasibility or technical study, including a cost estimate, relating to a policy or project of the public body;
 - (i) a report on the results of field research undertaken before a policy proposal is formulated;
 - (j) a report of an external task force, committee, council or similar body that has been established to consider a matter and make a report or recommendations to a public body;
 - (k) a plan or proposal to establish a new program or to change a program, if the plan or proposal has been approved or rejected by the head of the public body;
 - (l) information that the head of the public body has cited publicly as the basis for making a decision or formulating a policy; or
 - (m) a decision, including reasons, that is made in the exercise of a discretionary power or an adjudicative function and that affects the rights of the applicant.
- (3) Subsection (1) does not apply to information in a record that has been in existence for 15 years or more.



30. Legal advice

- 30.** (1) The head of a public body may refuse to disclose to an applicant information
- (a) that is subject to solicitor and client privilege or litigation privilege of a public body; or
 - (b) that would disclose legal opinions provided to a public body by a law officer of the Crown.
- (2) The head of a public body shall refuse to disclose to an applicant information that is subject to solicitor and client privilege or litigation privilege of a person other than a public body.

31. Disclosure harmful to law enforcement

- 31.** (1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to
- (a) interfere with or harm a law enforcement matter;
 - (b) prejudice the defence of Canada or of a foreign state allied to or associated with Canada or harm the detection, prevention or suppression of espionage, sabotage or terrorism;
 - (c) reveal investigative techniques and procedures currently used, or likely to be used, in law enforcement;
 - (d) reveal the identity of a confidential source of law enforcement information or reveal information provided by that source with respect to a law enforcement matter;
 - (e) reveal law enforcement intelligence information;
 - (f) endanger the life or physical safety of a law enforcement officer or another person;
 - (g) reveal information relating to or used in the exercise of prosecutorial discretion;
 - (h) deprive a person of the right to a fair trial or impartial adjudication;
 - (i) reveal a record that has been confiscated from a person by a peace officer in accordance with an Act or regulation;



- (j) facilitate the escape from custody of a person who is under lawful detention;
 - (k) facilitate the commission or tend to impede the detection of an offence under an Act or regulation of the province or Canada;
 - (l) reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;
 - (m) reveal technical information about weapons used or that may be used in law enforcement;
 - (n) adversely affect the detection, investigation, prevention or prosecution of an offence or the security of a centre of lawful detention;
 - (o) reveal information in a correctional record supplied, implicitly or explicitly, in confidence; or
 - (p) harm the conduct of existing or imminent legal proceedings.
- (2) The head of a public body may refuse to disclose information to an applicant if the information
- (a) is in a law enforcement record and the disclosure would be an offence under an Act of Parliament;
 - (b) is in a law enforcement record and the disclosure could reasonably be expected to expose to civil liability the author of the record or a person who has been quoted or paraphrased in the record; or
 - (c) is about the history, supervision or release of a person who is in custody or under supervision and the disclosure could reasonably be expected to harm the proper custody or supervision of that person.
- (3) The head of a public body shall not refuse to disclose under this section
- (a) a report prepared in the course of routine inspections by an agency that is authorized to enforce compliance with an Act; or
 - (b) a report, including statistical analysis, on the degree of success achieved in a law enforcement program unless disclosure of the report could reasonably be expected to interfere with or harm the matters referred to in subsection (1) or (2); or
 - (c) statistical information on decisions to approve or not to approve prosecutions.



32. Confidential evaluations

32. The head of a public body may refuse to disclose to an applicant personal information that is evaluative or opinion material, provided explicitly or implicitly in confidence, and compiled for the purpose of

- (a) determining suitability, eligibility or qualifications for employment or for the awarding of contracts or other benefits by a public body;
- (b) determining suitability, eligibility or qualifications for admission to an academic program of an educational body;
- (c) determining suitability, eligibility or qualifications for the granting of tenure at a post-secondary educational body;
- (d) determining suitability, eligibility or qualifications for an honour or award to recognize outstanding achievement or distinguished service; or
- (e) assessing the teaching materials or research of an employee of a post-secondary educational body or of a person associated with an educational body.

33. Information from a workplace investigation

33. (1) For the purpose of this section

- (a) "harassment" means comments or conduct which are abusive, offensive, demeaning or vexatious that are known, or ought reasonably to be known, to be unwelcome and which may be intended or unintended;
- (b) "party" means a complainant, respondent or a witness who provided a statement to an investigator conducting a workplace investigation; and
- (c) "workplace investigation" means an investigation related to
 - (i) the conduct of an employee in the workplace,
 - (ii) harassment, or
 - (iii) events related to the interaction of an employee in the public body's workplace with another employee or a member of the public

which may give rise to progressive discipline or corrective action by the public body employer.



(2) The head of a public body shall refuse to disclose to an applicant all relevant information created or gathered for the purpose of a workplace investigation.

(3) The head of a public body shall disclose to an applicant who is a party to a workplace investigation the information referred to in subsection (2).

(4) Notwithstanding subsection (3), where a party referred to in that subsection is a witness in a workplace investigation, the head of a public body shall disclose only the information referred to in subsection (2) which relates to the witness' statements provided in the course of the investigation.

34. Disclosure harmful to intergovernmental relations or negotiations

34. (1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm the conduct by the government of the province of relations between that government and the following or their agencies:

- (i) the government of Canada or a province,
- (ii) the council of a local government body,
- (iii) the government of a foreign state,
- (iv) an international organization of states, or
- (v) the Nunatsiavut Government; or

(b) reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies.

(2) The head of a public body shall not disclose information referred to in subsection (1) without the consent of

- (a) the Attorney General, for law enforcement information; or
- (b) the Lieutenant-Governor in Council, for any other type of information.

(3) Subsection (1) does not apply to information that is in a record that has been in existence for 15 years or more unless the information is law enforcement information.



35. Disclosure harmful to the financial or economic interests of a public body

35. (1) The head of a public body may refuse to disclose to an applicant information which could reasonably be expected to disclose

- (a) trade secrets of a public body or the government of the province;
- (b) financial, commercial, scientific or technical information that belongs to a public body or to the government of the province and that has, or is reasonably likely to have, monetary value;
- (c) plans that relate to the management of personnel of or the administration of a public body and that have not yet been implemented or made public;
- (d) information, the disclosure of which could reasonably be expected to result in the premature disclosure of a proposal or project or in significant loss or gain to a third party;
- (e) scientific or technical information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee of priority of publication;
- (f) positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the government of the province or a public body, or considerations which relate to those negotiations;
- (g) information, the disclosure of which could reasonably be expected to prejudice the financial or economic interest of the government of the province or a public body; or
- (h) information, the disclosure of which could reasonably be expected to be injurious to the ability of the government of the province to manage the economy of the province.

(2) The head of a public body shall not refuse to disclose under subsection (1) the results of product or environmental testing carried out by or for that public body, unless the testing was done

- (a) for a fee as a service to a person or a group of persons other than the public body;
- or
- (b) for the purpose of developing methods of testing.



36. Disclosure harmful to conservation

36. The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to result in damage to, or interfere with the conservation of

- (a) fossil sites, natural sites or sites that have an anthropological or heritage value;
- (b) an endangered, threatened or vulnerable species, sub-species or a population of a species; or
- (c) a rare or endangered living resource.

37. Disclosure harmful to individual or public safety

37. (1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, where the disclosure could reasonably be expected to

- (a) threaten the safety or mental or physical health of a person other than the applicant; or
- (b) interfere with public safety.

(2) The head of a public body may refuse to disclose to an applicant personal information about the applicant if the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's safety or mental or physical health.

38. Disclosure harmful to labour relations interests of public body as employer

38. (1) The head of a public body may refuse to disclose to an applicant information that would reveal

- (a) labour relations information of the public body as an employer that is prepared or supplied, implicitly or explicitly, in confidence, and is treated consistently as confidential information by the public body as an employer; or
- (b) labour relations information the disclosure of which could reasonably be expected to



(i) harm the competitive position of the public body as an employer or interfere with the negotiating position of the public body as an employer,

(ii) result in significant financial loss or gain to the public body as an employer, or

(iii) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer, staff relations specialist or other person or body appointed to resolve or inquire into a labour relations dispute, including information or records prepared by or for the public body in contemplation of litigation or arbitration or in contemplation of a settlement offer.

(2) Subsection (1) does not apply where the information is in a record that is in the custody or control of the Provincial Archives of Newfoundland and Labrador or the archives of a public body and that has been in existence for 50 years or more.

39. Disclosure harmful to business interests of a third party

39. (1) The head of a public body shall refuse to disclose to an applicant information

(a) that would reveal

(i) trade secrets of a third party, or

(ii) commercial, financial, labour relations, scientific or technical information of a third party;

(b) that is supplied, implicitly or explicitly, in confidence; and

(c) the disclosure of which could reasonably be expected to

(i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,

(ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,

(iii) result in undue financial loss or gain to any person, or

(iv) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

(2) The head of a public body shall refuse to disclose to an applicant information that was obtained on a tax return, gathered for the purpose of determining tax liability or collecting a



tax, or royalty information submitted on royalty returns, except where that information is non-identifying aggregate royalty information.

(3) Subsections (1) and (2) do not apply where

(a) the third party consents to the disclosure; or

(b) the information is in a record that is in the custody or control of the Provincial Archives of Newfoundland and Labrador or the archives of a public body and that has been in existence for 50 years or more.

40. Disclosure harmful to personal privacy

40. (1) The head of a public body shall refuse to disclose personal information to an applicant where the disclosure would be an unreasonable invasion of a third party's personal privacy.

(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy where

(a) the applicant is the individual to whom the information relates;

(b) the third party to whom the information relates has, in writing, consented to or requested the disclosure;

(c) there are compelling circumstances affecting a person's health or safety and notice of disclosure is given in the form appropriate in the circumstances to the third party to whom the information relates;

(d) an Act or regulation of the province or of Canada authorizes the disclosure;

(e) the disclosure is for a research or statistical purpose and is in accordance with section 70;

(f) the information is about a third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff;

(g) the disclosure reveals financial and other details of a contract to supply goods or services to a public body;

(h) the disclosure reveals the opinions or views of a third party given in the course of performing services for a public body, except where they are given in respect of another individual;



- (i) public access to the information is provided under the *Financial Administration Act*;
- (j) the information is about expenses incurred by a third party while travelling at the expense of a public body;
- (k) the disclosure reveals details of a licence, permit or a similar discretionary benefit granted to a third party by a public body, not including personal information supplied in support of the application for the benefit;
- (l) the disclosure reveals details of a discretionary benefit of a financial nature granted to a third party by a public body, not including
- (i) personal information that is supplied in support of the application for the benefit, or
- (ii) personal information that relates to eligibility for income and employment support under the *Income and Employment Support Act* or to the determination of income or employment support levels; or
- (m) the disclosure is not contrary to the public interest as described in subsection (3) and reveals only the following personal information about a third party:
- (i) attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or
- (ii) receipt of an honour or award granted by or through a public body.
- (3) The disclosure of personal information under paragraph (2)(m) is an unreasonable invasion of personal privacy where the third party whom the information is about has requested that the information not be disclosed.
- (4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy where
- (a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;
- (b) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation;
- (c) the personal information relates to employment or educational history;



- (d) the personal information was collected on a tax return or gathered for the purpose of collecting a tax;
- (e) the personal information consists of an individual's bank account information or credit card information;
- (f) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations;
- (g) the personal information consists of the third party's name where
- (i) it appears with other personal information about the third party, or
- (ii) the disclosure of the name itself would reveal personal information about the third party; or
- (h) the personal information indicates the third party's racial or ethnic origin or religious or political beliefs or associations.
- (5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether
- (a) the disclosure is desirable for the purpose of subjecting the activities of the province or a public body to public scrutiny;
- (b) the disclosure is likely to promote public health and safety or the protection of the environment;
- (c) the personal information is relevant to a fair determination of the applicant's rights;
- (d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;
- (e) the third party will be exposed unfairly to financial or other harm;
- (f) the personal information has been supplied in confidence;
- (g) the personal information is likely to be inaccurate or unreliable;
- (h) the disclosure may unfairly damage the reputation of a person referred to in the record requested by the applicant;



- (i) the personal information was originally provided to the applicant; and
- (j) the information is about a deceased person and, if so, whether the length of time the person has been deceased indicates the disclosure is not an unreasonable invasion of the deceased person's personal privacy.

41. Disclosure of House of Assembly service and statutory office records

41. The Speaker of the House of Assembly, the officer responsible for a statutory office, or the head of a public body shall refuse to disclose to an applicant information

- (a) where its non-disclosure is required for the purpose of avoiding an infringement of the privileges of the House of Assembly or a member of the House of Assembly;
- (b) that is advice or a recommendation given to the Speaker or the Clerk of the House of Assembly or the House of Assembly Management Commission that is not required by law to be disclosed or placed in the minutes of the House of Assembly Management Commission; or
- (c) in the case of a statutory office as defined in the *House of Assembly Accountability, Integrity and Administration Act*, records connected with the investigatory functions of the statutory office.



RECORDS RETENTION AND DISPOSAL SCHEDULE AMENDMENTS

A records retention and disposal schedule (RRDS or schedule) prescribes records retention periods and disposal plans, can apply to records in any format and authorizes disposal of records in a legal manner.

The *Management of Information Act* requires the Government Records Committee (GRC) to make recommendations to the Minister to dispose of government records. The RRDS is the recommended tool used for the legal disposal of government records.

RRDS documents are often referred to during the lifecycle of records which must be maintained and updated after they have been approved by the Government Records Committee (GRC).

Maintaining and Amending Records Retention and Disposal Schedules (RRDS)

Updates to the RRDS can either require an amendment to an existing schedule or depending on the level of changes required a new one be created, superseding the old. In any event, it must be approved by the GRC.

Amendments are minor revisions to the schedule that does not alter the context of the schedule. Amendments include, but are not limited to:

- Increase or decrease the overall retention period
- Changes to final disposition
- Minor changes to Record Series Title or Description
- Minor changes to Program/Service Name or Functions
- Changes to ATIPP Exceptions
- Change in ownership in its entirety.
- Change in official media type

All amendments must be submitted using a *Memorandum for Amending a Records Retention and Disposal Schedule to the Government Records Committee* including a *Summary of Change(s)* and the newly amended schedule.



Government of Newfoundland and Labrador
Office of the Chief Information Officer

Schedules that require major revisions which alters the context of the schedule must be submitted as a new Records Retention and Disposal Schedule (RRDS), voiding the old. Major changes include, but are not limited to:

- Addition or deletion of a Record Series
- Addition or deletion of a Program/ Service or Function

If a schedule is no longer required because the program or function is no longer a mandate of Government, the originating department must submit a memo to the GRC indicating that the previously approved retention schedule is now void and can no longer be applied.

This document contains step-by-step instructions on how to transition instant message content to a record-keeping format from:

- Text Messaging (SMS, MMS or iMessage)
- BlackBerry Messenger (BBM)
- Skype for Business

Notes:

- Text Messaging includes messages sent via Short Message Service (SMS), Multimedia Messaging Service (MMS) or iMessage
- Copying, Pasting or Forwarding content
 - may not retain the date, time and author of the information when text is copied
 - may not copy complete conversation (select all vs. select each chat bubble separately)
- An **ellipse (...)** or **tap and hold** are often used by applications to provide a menu of more choices
- Taking a screen shot of the instant messaging conversation is also an option but should still be emailed, including typing the critical text from image.

Iris and Donna are having an instant messaging conversation, via Text Message or BBM when they realize that their conversation has evolved and now contains information that should be captured as a record.

Text Messaging (SMS, MMS or iMessage)

Step 1:

Open the conversation and then tap and hold the chat bubble you wish to copy text from. You may have to select each chat bubble that you want to include if there is no Select All option.

Step 2:

Choose **Copy**.

Step 3:

Open a New Email Message, **Tap and Hold** in the message body and select **PASTE**.

Step 4:

Send the email to all those that participated in the Text Message instant messaging conversation

BlackBerry Messenger (BBM)

Step 1:

Open the Conversation and then select your Menu button [may be BlackBerry logo, ellipse (...) or similar choice]

Step 2:

Choose **Copy Chat** or **Email Chat** (if selected email chat then skip to Step 4).

Step 3:

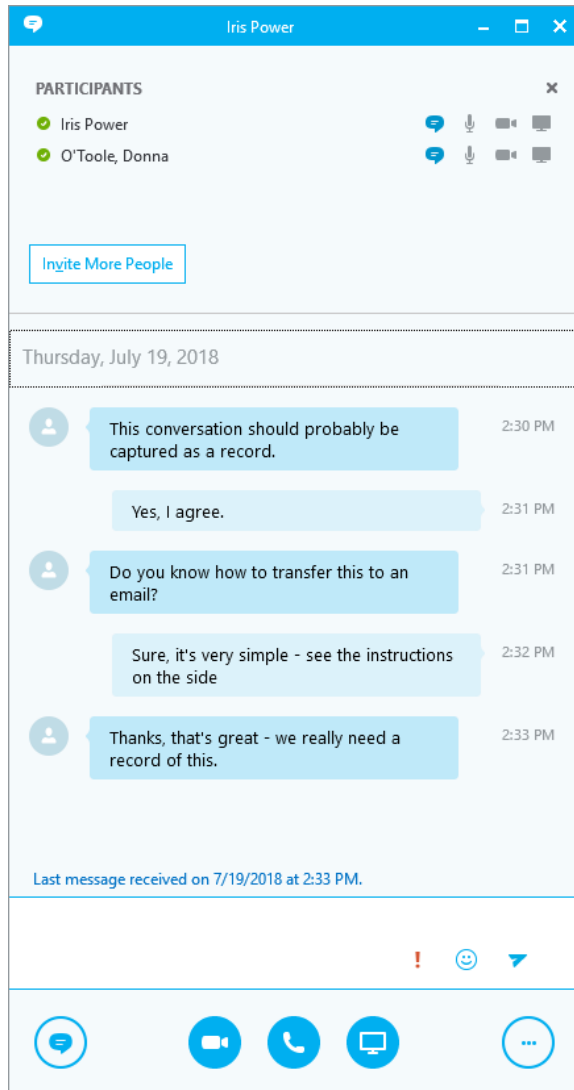
Open a New Email Message, **Tap and Hold** in the message body and select **PASTE**.

Step 4:

Send the email to all those that participated in the BBM instant messaging conversation.

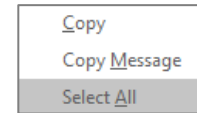
Skype for Business

Iris and Donna are having a conversation using Skype for Business when they realize that their conversation has evolved and contains information that should be captured as a record.



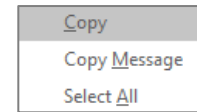
Step 1:

Right Click anywhere in conversation and choose **Select All**.



Step 2:

Right Click anywhere in conversation and choose **Copy**.



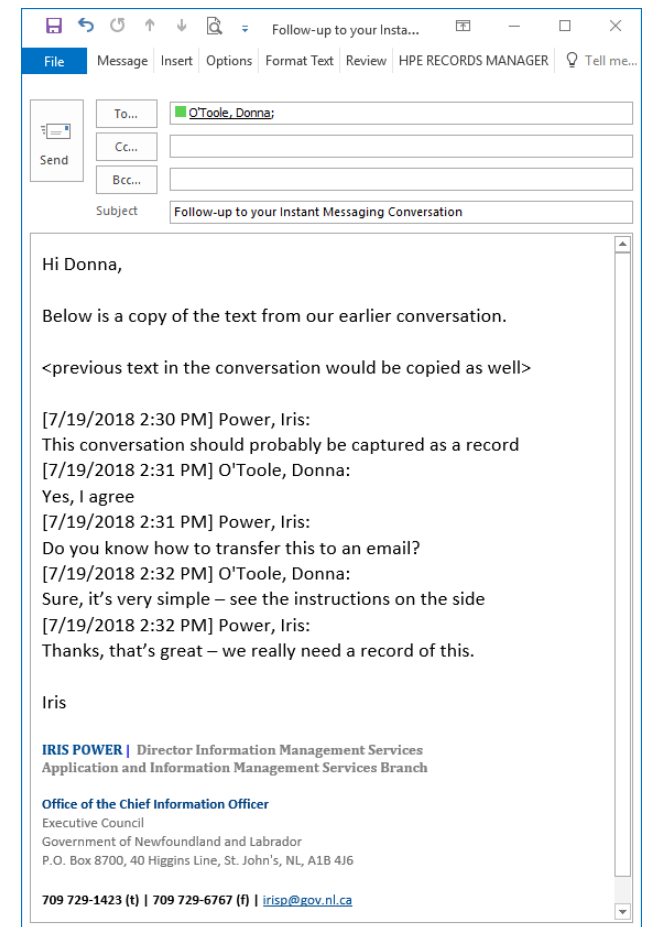
Step 3:

Open a New Email Message, **Right Click** in the message body and select **PASTE** (Keep Source Formatting, Merge Formatting or Keep Text Only).

We recommend using Keep Text Only when pasting from Skype for Business.

Step 4:

Send the email to all those that participated in the Skype for Business instant messaging conversation.





10. Templates

- 10.1. Records Retention and Disposal Schedule Template 1
- 10.2. Records Retention and Disposal Schedule Template 2
- 10.3. Memo – Request for Approval for RRDS for Submission to GRC
- 10.4. Memo – Request for Approval for RRDS Amendment
- 10.5. RRDS Amendment Summary of Changes
- 10.6. Memo – Notification of Ownership Change
- 10.7. One Time Disposal Submission Template
- 10.8. Memo – Approval for One Time Disposal Submission
- 10.9. Recordkeeping Guide



Government of Newfoundland and Labrador

RECORDS RETENTION AND DISPOSAL SCHEDULE (RRDS)

Insert name of Department or Public Body and Division

Date Last Updated: YYYY-MM-DD



Department or Public Body Name
 Division or Organizational Unit (If applicable)

RECORDS RETENTION AND DISPOSAL SCHEDULE

1.0 Overview

The Department of XYZ is responsible for.....

1.1 Administrative History

The Department of XYZ was...

1.2 Organizational Structure

Insert Organizational Chart

2.0 Abbreviations, Definitions & ATIPP Exceptions

ACT: Active	AR: Archival Retention	CY: Calendar Year	D: Destruction	DIS: Disposition
ED: Event Date	FY: Fiscal Year	N/A: Not applicable - this element does not apply.	PRD: Permanent Retention by Department	SA: Semi-Active
SR: Selective Retention	SO: Superseded/Obsolete	XYZ: Department of XYZ	-	-

ATIPP Exceptions

Section	Exception
27	Cabinet Confidences
28	Local public body confidences
29	Policy advice or recommendations
30	Legal advice
31	Disclosure harmful to law enforcement
32	Confidential Evaluations
33	Information from a workplace investigation



Department or Public Body Name
 Division or Organizational Unit (If applicable)

Section	Exception
34	Disclosure harmful to intergovernmental relations negotiations
35	Disclosure harmful to the financial or economic interests of a public body
36	Disclosure harmful to conservation
37	Disclosure harmful to individual or public safety
38	Disclosure harmful to labour relations interests of public body as employer
39	Disclosure harmful to business interests of a third party
40	Disclosure harmful to personal privacy
41	Disclosure of House of Assembly service and statutory office records
N/A	Not Applicable
Other	Other Federal or Provincial Acts or Regulations that prevail over ATIPP, or other Provincial Legislation that affects access.

3.0 Defining the Records Retention and Disposal Schedule

The Department of XYZ organizes records according to its classification plan based on the following levels:

1. Corporate Function / Primary Level: Describes the function or sub-function and summarizes any relevant information that impacts the creation, use, maintenance and disposition of its records. This would include any relevant legislation.
2. Secondary Level: Describes the records series including the type and format of information being captured, functions of the record, Office of the Primary Responsibility (OPR), retention policies and whether or not ATIPP exceptions would apply. *Remove this section if XYZ does not manage their records this way. You will also need to remove references to secondary levels under the main heading for sections 3.0 & 4.0.*

3.1 Defining Primary Levels

The primary levels are broken down by *<Insert how they are broken down (i.e functional entities)>* within XYZ.

Primary Level / Corporate Function	Definition



Department or Public Body Name
 Division or Organizational Unit (If applicable)

Primary Level / Corporate Function	Definition

3.2 Defining Secondaries

The following is a list of common and unique secondaries to XYZ. The common secondaries are based on the Corporate Records and Information Management Standard (C-RIMS). Unique secondaries are unique to the department or public body and should also be described below, if applicable. Include information specific to the division and the particular record series, where appropriate.

Common Secondaries	
Term	Definition
Policy, Standards, and Guidelines	Use for records relating to policy, standards or guidelines within any functional area.
Legislation	Use for records relating to acts and legislation. Departments are responsible for maintaining original documents pertaining to any provincial legislation administered by, or affecting the department. Any copies of federal legislation may be disposed of when no longer required by a department.
Agreements and Contracts	Use for agreements, contracts, memoranda of understanding, service level agreements and any other instrument which binds a department into an arrangement and/or partnership with another party.
Associations and Conferences	Use for records relating to associations, clubs, federations, foundations, leagues, societies and other organizations. Includes information about conferences, symposiums and other similar activities. Examples: proceedings, membership information, inquiries, solicitations.
Complaints	Use for complaints of any kind; match the Secondary with an appropriate functional area (Primary) as appropriate. For example, complaint to the Deputy Minister may be classified under the Executive Functions Primary as <i>Executive Functions-Complaints</i>
Planning	Use for records related to planning at the departmental, branch or divisional levels. Each type of plan should be handled separately.
Orders and Directives	Use for general orders and directives from Government central agencies (eg., Cabinet Secretariat, Treasury Board, Government Purchasing Agency); directives within departments (eg., Executive Directives); or circulars from the Department of Finance
Reports	Results of research or an account of past or projected organizational activity; may include statements of the organization’s plans, opinions, resources, etc.
Forms and Templates	Use for the management of government forms and templates employed with any internal or external government program and/or service.
Inter-departmental Committee	<Insert scope note here>



Department or Public Body Name
 Division or Organizational Unit (If applicable)

Common Secondaries	
Term	Definition
Departmental Standing Committee (eg., Executive Committee)	<Insert scope note here>
Steering Committee (eg., Project Steering Committee)	<Insert scope note here>
Ad Hoc Departmental Committee (eg., Committee established to address a specific topic or issue)	<Insert scope note here>
Working Group	<Insert scope note here>
Unique Secondaries	
Term	Definition
<Insert unique secondary here>	<Insert scope note here>
<Insert unique secondary here>	<Insert scope note here>

4.0 Records Retention and Disposal Schedule

The records retention and disposal schedule (RRDS or schedule) outlined below prescribes records retention periods and disposal plans for XYZ for the following formats: <insert all applicable formats here>.

4.1 ## - Corporate Function/Primary Level: <Insert the classification number, if applicable, and title of Corporate Function/Primary Level here>

The XYZ.... <Insert scope notes here for corporate function/primary level and identify vital records>.

Secondary Levels						
Term	Description	OPR	ACT	SA	DIS	ATIPP or Other Exceptions

Note:

- *OPR – OPR is ...
- *ED - Event date is...



Department or Public Body Name
 Division or Organizational Unit (If applicable)

4.2 ## - Corporate Function/Primary Level: <Insert the classification number, if applicable, and title of Corporate Function/Primary Level here>

The XYZ.... <Insert scope notes here for corporate function/primary level and identify vital records >.

Secondary Levels						
Term	Description	OPR	ACT	SA	DIS	ATIPP or Other Exceptions

Note:

*OPR – *OPR is...*

*ED - *Event date is...*



Department or Public Body Name
 Division or Organizational Unit (If applicable)

Records Retention and Disposal Schedule *Template*

Business Unit:		
Overview of Business Unit:		
Record Series Title:		
Record Series Description:		
Office of Primary Responsibility (OPR):		
Vital Record: <i>(Briefly Explain)</i>		
Identification of ATIPP and other Exceptions to Access as Applicable: <ul style="list-style-type: none"> <input type="checkbox"/> Not Applicable <i>(Rationale must be provided if not applicable is selected)</i> <input type="checkbox"/> Section 27 - Cabinet confidences <input type="checkbox"/> Section 28 - Local public body confidences <input type="checkbox"/> Section 29 - Policy advice or recommendations <input type="checkbox"/> Section 30 - Legal advice <input type="checkbox"/> Section 31 - Disclosure harmful to law enforcement <input type="checkbox"/> Section 32 - Confidential evaluations <input type="checkbox"/> Section 33 - Information from a workplace investigation <input type="checkbox"/> Section 34 - Disclosure harmful to intergovernmental relations negotiations <input type="checkbox"/> Section 35 - Disclosure harmful to the financial or economic interests of a public body <input type="checkbox"/> Section 36 - Disclosure harmful to conservation <input type="checkbox"/> Section 37 - Disclosure harmful to individual or public safety <input type="checkbox"/> Section 38 - Disclosure harmful to labour relations interests of public body as employer <input type="checkbox"/> Section 39 - Disclosure harmful to business interests of a third party <input type="checkbox"/> Section 40 - Disclosure harmful to personal privacy <input type="checkbox"/> Section 41 - Disclosure of House of Assembly service and statutory office records <p>Other: Identify Federal or Provincial Acts or Regulations that prevail over ATIPP, or other Provincial Legislation that affects access.</p> <p>**Records being transferred to <i>The Rooms Provincial Archives</i> may be made available to the public.</p> <p>Is there any issue with this information being made available to the public? <i>(If Yes, briefly explain)</i></p>		
Active (ACT)	Semi-Active (SA)	Disposition (DIS)

Memorandum

To: Chair, Government Records Committee

CC: Departmental or Public Body Information Manager, if an ADM or equivalent makes the submission cc the Deputy Minister

From: Deputy Minister, Assistant Deputy Minister or equivalent

Date: 2019-07-17

Re: Request for Approval of Operational Records Retention and Disposal Schedules

The (Department or Public Body Name) requests the approval of the Government Records Committee (GRC) to implement the attached Records Retention and Disposal Schedule (RRDS) for title of RRDS.

(Responsibility for the development and ongoing operation of IM activities has been assigned to (Departmental or Public Body Information Manager Name), the (Position Title). (Departmental or Public Body Access to Information and Protection of Privacy (ATIPP) Coordinator Name and Position Title) is responsible for the implementation of ATIPP for the (Department Name). The (Department or Public Body Name) will notify the Government Records Committee in the event that there is a change in resources.

This schedule has been reviewed for legal (ATIPP), financial, audit and operational requirements.

Please forward inquiries related to the use of the attached RRDS to:

Departmental or Public Body Information Manager Name	Departmental or Public Body ATIPP Coordinator
Mailing Address	Mailing Address
Phone Number	Phone Number
Fax Number	Fax Number
E-mail Address	E-mail Address

Sincerely,
Authorized Signing Officer

Memorandum

To: Chair, Government Records Committee

CC: [Departmental or other Public Body Manager responsible for IM, if an ADM or equivalent makes the submission cc the Deputy Minister or equivalent]

From: [Deputy Minister, Assistant Deputy Minister or equivalent]

Date: [month day, year]

Re: Request for Approval of Amendment to Operational Records Retention and Disposal Schedules (RRDS)

The [Department or Public Body Name] requests the approval of the Government Records Committee (GRC) to implement the attached amendment to Records Retention and Disposal Schedule (RRDS) [Retention Schedule Number – Title], previously approved by the Government Records Committee (GRC).

Responsibility for the development and ongoing operation of IM activities has been assigned to [Department or other Public Body Manager responsible for IM Name], [Position Title]. [Department or other Public Body Access to Information and Protection of Privacy (ATIPP) Coordinator Name] and [Position Title] is responsible for the implementation of ATIPP for the [Department or other Public Body Name]. The [Department or other Public Body Name] will notify the Government Records Committee in the event that there is a change in resources.

This schedule has been reviewed for legal (ATIPP), financial, audit and operational requirements.

Please forward inquiries related to the use of the attached RRDS to:

Manager responsible for IM	ATIPP Coordinator
[name]	[name]
[title]	[title]
[phone]	[phone]
[email]	[email]

Sincerely,

[Authorized Signing Officer Name]

[Authorized Signing Officer Title]

Attachments:

1. RRDS Amendment – Summary of Changes
2. Amended Records Retention and Disposal Schedule (RRDS)



Department or Public Body Name
 Division or Organizational Unit (If applicable)

Records Retention and Disposal Schedule (RRDS) Amendment

Summary of Changes

Retention Schedule Number: <Insert RRDS # here RS YYYY-###>				
RRDS Title: <Insert RRDS Title here >				
<p>Reason for Amendment: (Tick all that apply)</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <input type="checkbox"/> Change to Record Series Title or Description <input type="checkbox"/> Change to Program/Service Name or Function <input type="checkbox"/> Change to ATIPP exceptions <input type="checkbox"/> Other _____ </td> <td style="width: 50%; vertical-align: top;"> <input type="checkbox"/> Change in final disposition(s) <input type="checkbox"/> Change in retention period(s) <input type="checkbox"/> Transfer of ownership </td> </tr> </table>			<input type="checkbox"/> Change to Record Series Title or Description <input type="checkbox"/> Change to Program/Service Name or Function <input type="checkbox"/> Change to ATIPP exceptions <input type="checkbox"/> Other _____	<input type="checkbox"/> Change in final disposition(s) <input type="checkbox"/> Change in retention period(s) <input type="checkbox"/> Transfer of ownership
<input type="checkbox"/> Change to Record Series Title or Description <input type="checkbox"/> Change to Program/Service Name or Function <input type="checkbox"/> Change to ATIPP exceptions <input type="checkbox"/> Other _____	<input type="checkbox"/> Change in final disposition(s) <input type="checkbox"/> Change in retention period(s) <input type="checkbox"/> Transfer of ownership			
Summary of Changes:				
Item #	Detail Necessary Change	Reason for Change		
1				
2				
3				
4				
5				
6				

Note: Remember to attach the updated version of the Records Retention and Disposal Schedule (RRDS) that has the above noted changes incorporated.

Government of Newfoundland and Labrador

[Insert Name of Department]

[Insert Name of Branch or Division]

July 17, 2019

Chair
Government Records Committee
PO Box 8700
St. John's, NL
A1B 4J6

To whom it may concern:

Subject: Notification of Ownership Change

The Department of XXX wishes to notify you that as per (I.E. Order in Council, OC) the function of ZZ will now be administrated by the Department of YYY. This change is effective (Date) and control and custody of (active and semi-active) records will now be administered by YYY.

As a result, the following Records Retention Schedules, One Time Disposals and other affected documentation will be required to be updated to reflect the change.

1. RS Number:
2. DS Number:
3. CRIMS Approval Number:

This notification is provided to satisfy *the Management of Information Act, s.6 (1)*.

Please be advised at this time, this change (will/will not) include all structured electronic records systems designed to support this function. In the event of any further changes in custody as a result of the above directive, this Department will provide a supplementary update.

Sincerely,

Deputy Minister

cc: Deputy Minister
Department of YYY
Director, The Rooms Provincial Archives

Section 5.1 of the *Management of Information Act* provides the authority for the destruction of records through the Government Records Committee.

Section 5.2 of the *Management of Information Act* gives authority to the department to destroy records upon approval of a retention schedule.



*Department or Public Body Name
Division or Organizational Unit (If applicable)*

One Time Disposal Submission

DEPARTMENTAL/PUBLIC BODY USE	
Number of Boxes:	Box Numbers (Range):
Record Series Title:	
Records Created By Department/Public Body/ Branch /Division:	File Date Range: (YYYY-MM to YYYY-MM)
	Records Custodian:
	Email Address :
Phone No.:	

Departmental or Public Body ATIPP Coordinator:
<p>Identification of ATIPP and other Exceptions to Access as Applicable:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Not Applicable <input type="checkbox"/> Section 27 - Cabinet Confidences <input type="checkbox"/> Section 28 - Local public body confidences <input type="checkbox"/> Section 29 - Policy advice or recommendations <input type="checkbox"/> Section 30 - Legal advice <input type="checkbox"/> Section 31 - Disclosure harmful to law enforcement <input type="checkbox"/> Section 32 - Confidential evaluations <input type="checkbox"/> Section 33 - Information from a workplace investigation <input type="checkbox"/> Section 34 - Disclosure harmful to intergovernmental relations or negotiations <input type="checkbox"/> Section 35 - Disclosure harmful to the financial or economic interests of a public body <input type="checkbox"/> Section 36 - Disclosure harmful to conservation <input type="checkbox"/> Section 37 - Disclosure harmful to individual or public safety <input type="checkbox"/> Section 38 - Disclosure harmful to labour relations of a public body as employer <input type="checkbox"/> Section 39 - Disclosure harmful to business interests of a third party <input type="checkbox"/> Section 40 - Disclosure harmful to personal privacy <input type="checkbox"/> Section 41 - Disclosure of House of Assembly service and statutory office records <p>Note: Identify below Federal or Provincial Acts, Regulations or Departmental Public Access Restrictions that are applicable:</p> <p>**Records being transferred to <i>The Rooms Provincial Archives</i> may be made available to the public.</p>

NOTE - Records management forms are available on the [OCIO website](#) and can be downloaded or completed on-line for printing. Handwritten forms will no longer be accepted.

Please forward completed form to the Government Records Lifecycle Management Unit

Memorandum

To: Chair, Government Records Committee

CC: Departmental or Public Body Information Manager, if an ADM or equivalent makes the submission cc the Deputy Minister

From: Deputy Minister, Assistant Deputy Minister or equivalent

Date: 2019-07-18

Re: Request for Approval of One Time Disposal Submission

The (Department or Public Body Name) requests the approval of the Government Records Committee (GRC) of a One Time Disposal Submission

Records Series title:	Description:
-----------------------	--------------

(Responsibility for the development and ongoing operation of Information Management activities has been assigned to (Departmental or Public Body Information Manager Name), the (Position Title). (Departmental or Public Body Access to Information and Protection of Privacy (ATIPP) Coordinator Name and Position Title) is responsible for the implementation of ATIPP for the (Department or Public Body Name). The (Department or Public Body Name) will notify the Government Records Committee in the event that there is a change in resources.

This One Time Disposal Submission has been reviewed for legal (ATIPP), financial, audit and operational requirements.

Please forward inquiries related to the use of the attached One Time Disposal Submission to:

Departmental or Public Body Information Manager Name	Departmental or Public Body ATIPP Coordinator
Mailing Address	Mailing Address
Phone Number	Phone Number
Fax Number	Fax Number
E-mail Address	E-mail Address

Sincerely,
 Authorized Signing Officer

Authorized Individual's Name
Please Print

Authorized Signature

Position

Date

RECORDKEEPING GUIDE <TEMPLATE>	
Approval Date	<yyyy-mm-dd> (<i>Date of approval by final authority</i>)
Authorizing Body	e.g. Council, Committee, etc
APPROVAL AND SIGN OFF	
<Permanent Head>, <Public Body>	< signature >
	< name > < yyyy – mm – dd>
Additional Signing Authority may be needed depending on governance structure	< signature >
	< name > < yyyy – mm – dd>
Note: Questions related to this guide should be forwarded to IM@gov.nl.ca .	

TABLE OF CONTENTS

1.0 Overview1

2.0 Purpose.....1

3.0 Scope1

4.0 Background1

 4.1 Government Versus Transitory Records 1

 4.2 Effective Records Management.....2

5.0 Employee Orientation3

 5.1 New Employees, IM Responsibilities3

6.0 Recordkeeping Requirements.....4

 6.1 Collection, Creation and Receipt4

 6.1.1 Record Content.....4

 6.1.2 Email Use.....4

 6.1.3 Meeting Management4

 6.2 Organization and Storage4

 6.2.1 Organization of Records4

 6.2.2 Authorized storage locations5

 6.2.3 Portable Storage Devices5

 6.3 Sharing and Use5

 6.3.1 Collaboration.....5

 6.3.2 Appropriate Disclosure.....5

 6.3.3 Safe Business Practices5

 6.4 Disposal6

 6.4.1 Secure Destruction6

7.0 Definitions and Acronyms6

 7.1 Definitions6

8.0 Monitoring and Review6

9.0 References.....7

10.0 Appendices.....8

 10.1 Appendix A: Sample 1: Meeting Agenda9

 10.2 Appendix B: Sample 2: Meeting Minutes 10

 10.3 Appendix C: Sample 3: Meeting Minutes..... 11

 10.4 Appendix D: Template – Record Keeping Checklist..... 12

RECORDKEEPING GUIDE

1.0 Overview

Public bodies require records to demonstrate compliance, transparency and accountability. Because ABCs are often accountable to another public body/ABC, they must meet common operating and reporting requirements. There are a wide range of ABCs working to support public policy, programs and services across Newfoundland and *The Management of Information Act (MOIA)* mandates that public bodies implement an Information Management (IM) program to manage records of all media. This recordkeeping guide outlines requirements for individuals engaged to perform work on behalf of a public body.

The OCIO's list of *public bodies* provides an overview of agencies, board and commissions across government.

2.0 Purpose

This guideline provides individuals with recordkeeping requirements that should be followed when handling records and information on behalf of a public body.

3.0 Scope

This Guideline applies to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of a public body (hereafter referred to as individuals).

4.0 Background

4.1 Government Versus Transitory Records

The *MOIA* mandates that each public body have an IM program. While overall accountability for IM rests with the permanent head of a public body, individuals must ensure the business activities they complete on behalf of government are recorded, managed and protected. The *MOIA* contains the following definitions for records:

Record – A record means a correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic

Government Record - A record created by or received by a public body in the conduct of its affairs and includes a Cabinet record, transitory record and an abandoned record.

The disposal of a government record must be authorized by the Government Records Committee (GRC) and documented as a part of the IM program's requirements. The additional steps required to dispose of a government record ensure 1) disposal is legal and authorized and 2) no known legal issues require the disposal be delayed until it is resolved.

In today's technological work environment, information is easily generated, shared and stored as part of their normal business in multiple locations. Individuals often decide how/if records will be retained and disposed of (e.g., email messages). Multiple versions of information are retained in email in/outboxes and on network or personal file shares which may not be appropriate.

The *MOIA* includes the following definition:

Transitory Record - A government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

The *MOIA* encourages the ongoing secure destruction of transitory records:

Transitory records may be disposed of when they are no longer of value, and shall only be disposed of through means which render them unreadable, including secure shredding or in the case of electronic records, secure electronic erasure.

Government records, as in the definition above, includes any media capable of capturing information including paper records, electronic records, email messages, system data, etc. may constitute a government record. The value of records is dependent on its significance to the event, transaction, activity or process to which it relates and not to its format.

Identifying a record as transitory means, it has no legal or operational value. It does not mean content is not valuable or potentially contain personal or confidential information. This is why safe handling and secure destruction are required.

4.2 Effective Records Management

Include a summary of the public body's mandate, organizational structure, operational requirements, etc. as necessary to put records management into context.

As a public body, the entity must comply with the *MOIA*. Effective records management practices are important to administrative and operational functions. Some reasons for consistent and effective recordkeeping include but are not limited to:

- **Improved Decision-making:** Good records management ensures information needed to make decisions is more readily available.

- **Efficient Resource Usage:** Records cost money and time to store, process and maintain. Effective control means resources are used appropriately.
- **Improved Information Reuse and Collaboration:** Better control over records supports the ability to identify and reuse final versions.
- **Minimize Search and Retrieval Time:** Applying consistent rules around how records are organized and stored makes it easier to find information when needed.
- **Reduce Discovery Costs/Resources:** In the event of a discovery process including audit, inquiry, litigation or a request for information made under the *Access to Information and Protection of Privacy Act, 2015 (ATIPPA)* all information within the parameters of the request, regardless of its value, must be produced by the public body/ABC. Good records management practices make it easier to meet ATIPPA requirements.
- **Compliance with Legislative Requirements:** In addition the *MOIA*, public bodies must comply with many legal and regulatory requirements. Compliance is dependent on its ability to produce high-quality records that demonstrate how it met its mandate.
- **Penalties for Individuals Who Violate the *MOIA*:** The *MOIA* includes potential legal and financial penalties for individuals that violate it.

5.0 Employee Orientation

5.1 New Employees, IM Responsibilities

How new employees manage their records from day one can permit an organization to operate more effectively. A sample new employee checklist is included in Appendix D to assist public bodies with employee IM orientation.

Employees play a critical role in maintaining organizational records. To help new employees learn their IM responsibilities *IM@Work* is available to public bodies on the OCIO website. The course is designed to provide an introduction to IM and relevant legislation; review of information management best practices; and provide an overview of information management roles and responsibilities.

6.0 Recordkeeping Requirements

6.1 Collection, Creation and Receipt

6.1.1 Record Content

- Identify personal/confidential information the public body is authorized to collect
- List of the records typically created to support business processes
- Link to forms and templates

6.1.2 Email Use

- Describe how email is provided and used to support business processes
- Reiterate email is discoverable as part of an ATIPP request or legal action
- Include guidance on personal use and use of personal email accounts
- Refer to best practices on email phishing

6.1.3 Meeting Management

- Outline details for standing meetings – logistics, roles, etc. Consider OCIO guidance in the *Advisory - Meeting Records*.
- Include templates for agendas and minutes. Samples have been included in Appendices A, B and C.

6.2 Organization and Storage

6.2.1 Organization of Records

- Suggest an approach to organizing records to encourage consistency. For example:
 - Meeting records – Meeting date/Fiscal or Calendar Year
 - Case Files – Unique Identifier/Fiscal or Calendar Year

6.2.2 Authorized storage locations

- Identify where the record of authority is stored and how it is accessed for reference.
- Suggest organization for record types identified in 5.1.1.
- Identify any limitations on storage in personal or non-government work locations

6.2.3 Portable Storage Devices

- Promote use of encrypted portable storage devices to transport records

6.3 Sharing and Use

6.3.1 Collaboration

- Outline the preferred process to collaborate

6.3.2 Appropriate Disclosure

- Identify any restrictions on access
- Identify what needs to happen when an access request is made

6.3.3 Safe Business Practices

- Refer to points in OCIO FYI's relevant to the public body's processes
- If provided with access to the Government Network Link to the OCIO Directive - *Acceptable Use of the Government Network and Information Technology Assets*

6.4 Disposal

6.4.1 Secure Destruction

- Outline what happens to the record of authority and what happens to the transitory records retained by the individual
- Identify timeframe for retention of official records
- Refer to points in OCIO FYI’s relevant to the public body’s processes
- Return to public body or to the department (reporting entity) for secure destruction is an option

7.0 Definitions and Acronyms

7.1 Definitions

Transitory Record

Information Management

Acronyms

ATIPPA	Access to Information and Protection of Privacy Act, 2015
IM	Information Management
MOIA	<i>Management of Information Act</i>

8.0 Monitoring and Review

Identify who will be responsible for keeping the document up to date and monitoring compliance.

9.0 References

Links to all published information referenced in the document including:

Management of Information Act

OCIO Directive

Acceptable Use of the Government Network and Information Technology Assets

OCIO Directive

Instant Messaging

OCIO Quick Reference

USB Flash Drives: What You Should Know

OCIO Advisory

Meeting Records

OCIO Advisory

Case Files

10.0 Appendices

10.1 Appendix A: Sample 1: Meeting Agenda

This template is provided as a sample to be modified as required

<Public Body Logo> <Public Body Name>
<Public Body Division Name>

MEETING AGENDA

Objective	
Meeting Date	
Meeting Time	
Meeting Location	
Chair	
Participants	

	Topic
1.	
2.	
3.	
4.	
5.	
6.	Action Items
7.	Next Meeting

10.2 Appendix B: Sample 2: Meeting Minutes

This template is provided as a sample to be modified as required

<Public Body Logo>

<Public Body Name>

<Public Body Division Name>

MEETING MINUTES

Meeting Date	
Meeting Time	
Meeting Location	
Participants	Name, Organization, Role
Regrets	Name, Organization, Role

	Topic	Notes
1.		
2.		
3.		
4.	Action Items	
5.	Next Meeting	

	Action Items	Resource Name	Status/Timeline
1.			
2.			
3.			
4.			
5.			

10.3 Appendix C: Sample 3: Meeting Minutes

This template is provided as a sample to be modified as required

Public Body Logo

Public Body Name

TITLE/SUBJECT MEETING

DATE

LOCATION

TIME

MINUTES OF MEETING

Attendance:

Identify all persons in attendance, their title, organization and role

Identify all persons that have sent regrets, their title, organization and role

1. Call Meeting to Order
2. Approval of minutes from the last meeting
3. Business arising from last meeting minutes
4. New Business
5. Action Items
 - Provide a listing of actions items with resources assigned, timelines, etc. if relevant
6. Next Meeting and Adjournment
 - Set time, date location, etc. if possible

10.4 Appendix D: Template – Record Keeping Checklist

New Employee/Individual Record Keeping Checklist Template

Using a checklist when providing orientation to a new employee or individual engaged to perform work on behalf of the Agency, Board or Commission (ABC) may be helpful in ensuring all elements are communicated and understood.

Checklist items are based on the content of the ABC's record keeping guide. As such, each checklist will reflect the ABC's unique requirements. The following list includes common elements that may be discussed when a new individual is engaged to perform work on behalf of the ABC.

Elements may be deleted/added as required.

- IM@Work - Review the document on the OCIO website will provide a general overview of Information Management (IM), The Management of Information Act (MOIA), individual responsibilities, and best practices.
- List of personal or confidential information collected/maintained (if relevant)
- Identify known records to be created/maintained by the individual
- Identify forms/templates to be used and where they are located
- Review email usage requirements
- Review how/where records are organized/stored
- Allocate IT resources/equipment:
 - Laptop/personal computer
 - Tablet
 - Portable storage device
- Review disposal requirements

Please note there may be other additional orientation required (e.g. financial, privacy etc.)



Section C

GRC Role

Government Records Committee (GRC)

The Management of Information Act, section 5.1 (1) establishes the Government Records Committee (GRC) providing them with authority to:

- Establish and revise schedules for the retention, disposal, destruction or transfer of records
- Make recommendations to the Minister respecting government records to be forwarded to the archives
- Establish disposal and destruction standards and guidelines for the lawful disposal and destruction of government records
- Make recommendations to the Minister regarding the removal, disposal and destruction of records

Membership

- Director of The Rooms Provincial Archives
- Deputy Minister of Justice or designate
- Deputy Minister of Finance or designate
- Chief Information Officer or designate
- Other persons whom the Minister, appointed under the Executive Council Act, may appoint

Note: The Chief Information Officer or designate is the chair of the GRC with the OCIO



Section D

PRC Storage

Provincial Records Centre (PRC) Storage

Operated by the Office of the Chief Information Officer (OCIO) under the Government Records Lifecycle Management (GRLM) program, the Provincial Records Centre (PRC) provides: a safe, secure storage facility for semi-active government records; support to the Government Records Committee (GRC); and guidance to public bodies on the appropriate disposal of government records.

Records storage is available to those public bodies whose information technology services are provided by the OCIO.

Criteria

The following classes of semi-active government records are eligible for storage at the PRC:

- Vital Records that are identified as either indispensable to a mission critical business operation or essential for the continuation of an organization during or following a disaster.
- Records for which the legal or operational needs of the department dictate that custody and/or control of the information must remain within government.
- Records which, due to their enduring value or historical significance, are to be transferred to The Rooms Provincial Archives Division when no longer required by the department or public body.
- Records which have longer than usual semi-active retention periods may be considered, to lessen the burden of storage costs on departments and public bodies.

- Records must have an approved Records Retention and Disposal Schedule.

PRC staff provides timely access to records in storage and facilitates the delivery and pick-up of records when needed. It is the responsibility of the requesting department to pay all costs associated with delivery and pick up requests. Access to records will only be given to individuals who have been authorized on the PRC Client Chart of Authority.

Current Records Inventory per Department

Below is a listing of records holdings at the PRC as of May, 2019.

Advanced Education, Skills and Labour	862
Tourism Culture Industry and Innovation	1,234
Child Seniors and Social Development	14
Executive Council (<i>includes Cab. Sec, HRS, OCIO, etc</i>)	882
Finance	241
Fisheries and Land Resources	320
Health and Community Services	937
Justice (<i>includes Courts</i>)	12,168
Service NL	894
The Rooms	12
Transportation and Works	282
Treasury Board	26
Total Records Holdings Inventory	17,872



Section E

Guide to IM for Public Bodies

1. Core IM Foundation	23
1.1. IM Governance, Accountability and Organization	
1.2. IM Vision, Mission and Guiding Principles	
1.3. IM Legal and Regulatory Framework	
1.4. IM Program Plan	
2. IM Program Components.....	28
2.1. Information Management Policy Instruments	
2.2. Information Management Performance Measurement	
2.3. Education and Awareness for IM Practitioners	
2.4. IM Education and awareness for Government Employees	
2.5. Physical Records Storage and Development and Use	
2.6. Information Protection	
3. IM Tools	35
3.1. Records and Information inventory	
3.2. Classification Plan Development for Operational records	
3.3. Records Classification Plan Implementation	
3.4. Disposal of Records	
3.5. Record Imaging Services	



1. Core IM Foundation

1.1. IM Governance, Accountability and Organization	24
1.2. IM Vision, Mission and Guiding Principles	25
1.3. IM Legal and Regulatory Framework.....	26
1.4. IM Program Plan	27



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – INFORMATION MANAGEMENT (IM) GOVERNANCE, ACCOUNTABILITY AND ORGANIZATION

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)** approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015 03 26
OCIO TRIM Number	DOC04992/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	
Related Guidelines	See References

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch	
	(name) (signature) (date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	1
2.0	Scope	1
3.0	Background	1
3.1	IM Governance Framework Components	2
3.1.1	Strategic Planning	3
3.1.2	Program Planning and Management.....	3
3.1.3	Program Administration	3
3.1.4	Program Instruments and Tools	4
3.1.5	Service Delivery.....	4
3.1.6	Practices	4
3.2	Accountability and Organization	5
4.0	Recommended Approach.....	5
4.1	Document the Departmental IM Governance Framework.....	5
4.2	Identify Staff Who Perform IM Functions.....	5
4.3	Map Existing IM Functions to Staff.....	6
4.4	Define the Accountability Structure	6
4.5	Document the IM Organizational Structure	7
4.5.1	Design Principles.....	7
4.5.2	Design Challenges	7
4.6	Obtain Approval.....	8
4.7	Education and Awareness.....	8
4.8	Review and Update	8
5.0	Glossary	9
5.1	Acronyms.....	9
6.0	References.....	9
7.0	Revision History	10
	Appendix A: Sample Information Management (IM) Roles and Responsibilities	11

INFORMATION MANAGEMENT (IM) GOVERNANCE, ACCOUNTABILITY AND ORGANIZATION GUIDELINE

1.0 Overview

An Information Management (IM) Governance Framework describes the actions supported by a department to meet IM legal, regulatory and operational requirements. Accountability and Organization are essential components of the Governance Framework. Accountability in this context includes the identification of the departmental roles and level of engagement required to ensure that the IM program operates effectively. Organization refers to the way that these responsibilities are allocated to individuals in the department. This guideline is designed to assist public bodies in the Government of Newfoundland and Labrador to develop an approach to IM Governance, Accountability and Organization

2.0 Scope

This Guideline applies to or may be used by all public bodies (hereafter referred to as departments), as defined in the *Management of Information Act*. The audience for this guideline includes all individuals responsible for the operation of an IM program within their department.

3.0 Background

The *Management of Information Act* (Section 6) mandates that a permanent head of a public body:

- Requires that each department develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records;
- Assigns overall accountability for the operation of an IM program to the Deputy Minister;
- Allocates responsibility for the management of government information to the individual employee.

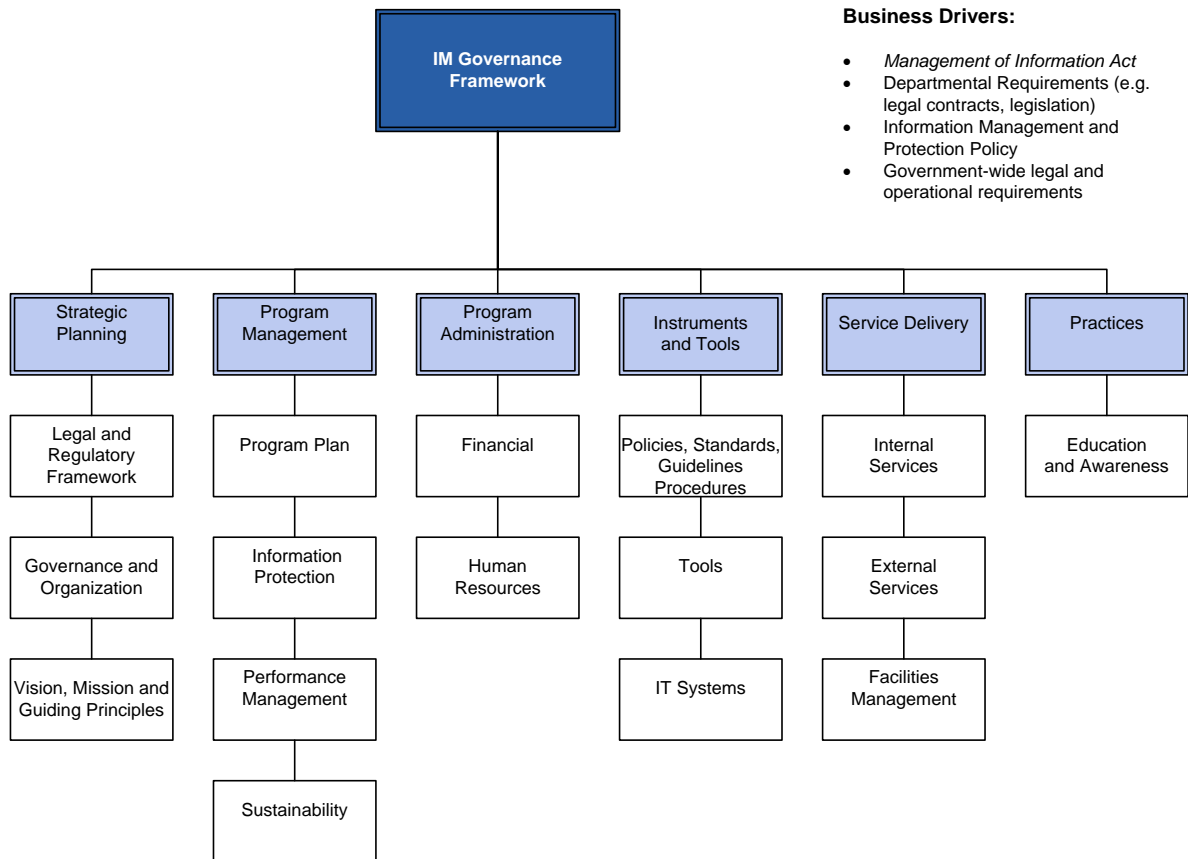
To ensure that these, and other, obligations are met, IM has been included as a requirement in Executive performance contracts. IM governance, accountability and organization:

- Enable the Deputy Minister or equivalent to properly discharge his or her responsibilities according to applicable legislative, regulatory and operational requirements;
- Ensure that the required policies, procedures, standards and guidelines are authorized and effectively used;
- Guide the development and ongoing operation of the IM program plan.

3.1 IM Governance Framework Components

The following diagram depicts the components of an IM Governance Framework. Note that this is not an organizational chart. The groupings link related functions to promote an overall understanding of how they may be interrelated in a department. How these functions are performed will vary depending on the size, scope and requirements of the department, available resources, etc. A single individual or grouping of individuals may be assigned to a particular function or to multiple related functions as required to meet both the business requirements and the budgetary and organizational realities within which it operates.

Figure 1: Sample Information Management (IM) Governance Framework



Guideline – Information Management (IM) Governance, Accountability and Organization

3.1.1 Strategic Planning

Strategic planning for IM is driven by the department's interpretation of how it will achieve compliance with its IM-related legal, regulatory and operational requirements. IM governance, accountability and organization described in this guideline provide a foundation for strategic planning. Also included are:

- **Legal and Regulatory Framework:** Legal and regulatory requirements are non-negotiable considerations that must be incorporated into the department's IM strategy. The OCIO Guideline *Information Management (IM) Legal and Regulatory Framework* details the development of legal and regulatory requirements for the IM program.
- **Vision, Mission and Guiding Principles:** Vision, mission and guiding principles state the foundation of what the IM program stands for and what it is designed to achieve. The OCIO Guideline *Information Management (IM) Vision, Mission and Guiding Principles* details the development of vision, mission and guiding principles.

3.1.2 Program Planning and Management

IM Program Planning and Management documents how IM capabilities and services are created, delivered and managed within the department. This includes:

- **Program Plan:** An Information Management (IM) Program Plan outlines how IM works in a department. The OCIO Guideline *Information Management (IM) Program Plan* details the development and implementation of an IM Program Plan.
- **Information Protection:** The OCIO Guideline *Information Protection* details the development and implementation of an information protection plan.
- **Performance Measurement:** Performance Measurement includes activities to ensure that goals are consistently being met in an effective and efficient manner. The OCIO Guideline *Information Management (IM) Performance Measurement* details the development and implementation performance benchmarks, metrics and reporting against the IM program plan.

3.1.3 Program Administration

IM Program Administration refers to the activities required by the department to maintain operations within the framework adhered to by the department as a whole. Financial management and human resource management are examples of these activities. Requirements including processes, approval and reporting requirements may be specific to the department or apply government-wide.

3.1.4 Program Instruments and Tools

IM Program Instruments and Tools are used to support the operation of IM within the department. These may include:

- The development of policies, standards, procedures and guidelines specific to IM-related activities. The OCIO Guideline *Information Management (IM) Policy Instruments* details the development, approval and implementation of IM-related instruments needs to support the IM Program.
- IM tools used to document and prescribe technical requirements for the management of information. Examples include Records Classification Plans, Records Retention and Disposal Schedules (RRDS) and Records and Information Inventories. Guidelines related to the development and information of IM tools are listed in the reference section of this document.
- Information Technology (IT) Systems are technology applications that are used to house, manage and dispose of government information and support business and decision-making. The TRIM Electronic Document and Records Management Systems (EDRMS) is an example of a system commonly used by departments to manage records. OCIO Guideline *IM Policy Instruments* details the development, approval and implementation of IM-related Systems.

3.1.5 Service Delivery

IM Service Delivery includes the IM-related activities that will be supported, both internally and externally, by IM staff identified in the organizational structure.

- Internal/External Services: The definition of IM Services is detailed in the OCIO Guideline *Information Management (IM) Program Plan*.
- Facilities: Facilities are the physical structures used by the department to support ongoing operations including the creation, receipt, storage and disposal of government information. Requirements for the operation of facilities are detailed in the OCIO Guideline *Physical Records Storage Development and Use*.

3.1.6 Practices

IM Practices include the way that employees support the department's IM Governance Framework. This includes both general employees and IM practitioners. IM education and awareness is used to ensure that employees have the information they need to meet their obligations; thereby improving overall departmental IM capacity. The OCIO Guidelines *Information Management (IM) Education and Awareness for Government Employees* and *Education and Awareness for IM Practitioners* provide information on the use of education and awareness to support IM practices.

3.2 Accountability and Organization

The *Management of Information Act* prescribes a high-level accountability for IM. Each department must determine how accountability will be assigned to ensure compliance with all IM-related requirements. IM accountability and organization are used to identify how and by whom the above described functions will operate within the department.

- Accountability Structure: Accountability includes the mapping of IM functions and level of engagement to specific departmental roles. Based on these roles and responsibilities, an organizational structure can be developed.
- Organizational Structure: Outlines the employees within the department's IM Program and their lines of reporting.

4.0 Recommended Approach

4.1 Document the Departmental IM Governance Framework

The components described in Section 3.1 of this document can be used as a basis for a departmental IM governance framework. Additional components may be required to accommodate department specific requirements. An Information Management Capacity Assessment Tool (IMCAT) final report and other existing documentation such as business plans and annual reports may be key inputs to this activity. Preparing a pictorial representation with descriptions as modeled in Section 3.1 will help to identify gaps. Compare what the department has with the categories identified in Section 3.1. Add to the model any descriptions and department specific functions.

4.2 Identify Staff Who Perform IM Functions

In order to develop IM accountability and organization structures, it is important to have a solid understanding of the staff available to perform the IM functions. Using the IM governance framework identified in Section 4.1, identify the departmental staff that currently performs functions. Note functions that do not have resources allocated. Include in this assessment:

- The Executive responsible for IM within the department
- Existing IM Staff including their current position scope and expectations
- Departmental staff who perform IM functions but may not have IM as their primary role (e.g., administrative support, policy analysts, etc.)
- Identify key resources on the periphery of IM practice within the department that must be engaged in certain activities including:
 - Legal counsel responsible for advice and guidance on IM-related issues including legislative and regulatory requirements for records retention and disposal.
 - Departmental Access to Information and Protection of Privacy (ATIPP) Coordinator who must be engaged in the operation of the IM program to identify ATIPP requirements in the development of program components (e.g. retention schedules, procedures, policies, etc.) and support ongoing processes including

Guideline – Information Management (IM) Governance, Accountability and Organization

records disposal. ATIPP staff will also use IM services in the processing of requests made under the ATIPP legislation.

4.3 Map Existing IM Functions to Staff

Based on the model and descriptions in 4.1, identify the IM functions that are currently staffed. Examine the existing functions to determine whether these staffing allocations are appropriate. Also identify functions of the IM program that are missing. Chances are these are areas that will require allocation of existing staff or new staff to fill the void. Use the IM position descriptions and technical competencies to identify the skills and resources required to fill gaps. Copies of this information are located in on the [OCIO Website](#).

4.4 Define the Accountability Structure

The IM accountability structure identifies who is engaged in each IM function and at what level. This differs from the organizational structure because it identifies numerous resources engaged in operations other than IM (e.g., legal counsel).

- Deputy Minister/Executive
- Director of Information Management
- Departmental Advisors to IM including Legal Counsel, and departmental ATIPP Coordinator
- IM Practitioners including managers, analysts and technicians
- Functional Director/Manager(s)
- Administrative support
- Employees

Roles and responsibilities link specific functions to employees. It is important to note that not some IM functions are performed traditionally by staff in other business roles. This does not mean that they need to be reclassified as IM staff. For example, administrative staff supports the implementation of TRIM for Executive correspondence management because they are responsible for that function as a part of the Executive and management support role. The role of IM in the department is to support these staff by ensuring that the appropriate training and support is available to them related to the use of TRIM, scanning best practices, etc.

A *Sample Roles and Responsibilities Chart* has been included in Appendix A. This tool is used to quickly identify the roles responsible for each function and their level of engagement. Departments may find it useful to start with this type of listing and then develop the detailed roles and responsibilities descriptions.

4.5 Document the IM Organizational Structure

The Organizational structure differs from the accountability model in that it identifies the way that IM staff is organized within the department. Staff identified in the organizational structure have IM functions within their position description and are primarily responsible for IM functions.

4.5.1 Design Principles

The following design principles are recommended in the development of the organizational structure:

- **IM Professional Management** - All IM staff should report to an IM Director or an IM Manager who can provide specialized IM management oversight and supervision;
- **IM Reporting** - The IM Director will report to the Deputy Minister or equivalent, who has overall accountability for IM under the *Management of Information Act*. If that is not feasible, then the IM Director should report to an Assistant Deputy Minister (or equivalent) responsible for Corporate Services. This ensures that IM is represented as an essential corporate service at the Executive level.
- **IM Competency Model** - The IM organizational structure should use the IM Competency Model and its standardized IM position specifications adopted by Government.
- **IM Resource Allocation** - The actual resourcing of the IM organization (numbers of IM staff members by position classification) will be dependent on the IM workload in the public body and the availability of resources, but should at least aim to have an appropriate balance between management level and non-management operational IM staff resources.

4.5.2 Design Challenges

The design of an IM organization for a department will be impacted by a number of challenges, including:

- **Business Complexity:** A department with multiple lines of business and a large geographic spread will have more complex IM challenges than a smaller one with fewer lines of business and located in a small number of locations.
- **Task Specialization:** Given that all of the tasks in the IM Functional Model need to be done, the more staff that are included in the IM organization means that task specialization will be easier, with one individual usually possessing a high level of expertise and experience. In smaller IM organizations, multi-tasking will be required, with a broader range of expertise and experience required of each individual. In many cases, a multi-tasked resource cannot have the same level of expertise and experience as a specialized resource.
- **Geographic Distribution:** Departments with offices and operations in more than one location face a greater IM supervisory challenge than those operating from one location.

Guideline – Information Management (IM) Governance, Accountability and Organization

- **Staff Involvement in IM:** In all of the models below as well as in actual practice across the Government of Newfoundland and Labrador, many non-IM staff perform IM functions, such as correspondence management. In these cases, the role for IM staff is to be a resource to assist the non-IM staff to perform IM functions. The IM staff can provide direction, assistance, advice and supervision of work as well as perform IM compliance checks.
- **Management Structure:** The management structure in a particular department will impact whether the senior IM position is an IM Director, a Manager or a bargaining unit position.
- **Support from OCIO** These models all reflect support from the OCIO in these areas:
 - **“External” IM Services** These are IM and IT services provided by the OCIO
 - Common IM services used across the Government
 - Common Government applications
 - Specific applications for individual public bodies that are provided and supported by the OCIO
 - **Information Management and Protection Advisory Services** These services provide specialized advice and assistance to public bodies on matters related to Information Management and Protection.

4.6 Obtain Approval

The IM governance framework and the, accountability and organizational structures must be reviewed as appropriate by departmental stakeholders as per established departmental protocols.

4.7 Education and Awareness

Education and awareness are essential for both departmental employees and for those staff that are classified as IM practitioners. All staff should be aware of the governance framework as well as the accountability and organizational structures. Departmental employees need to be aware of their role in IM and to understand the various services accessible to them. Ongoing education and awareness is also important for IM practitioners, especially those who may have been newly allocated or reclassified to an IM role. The OCIO Guidelines *Information Management (IM) Education and Awareness for Government Employees* and *Education and Awareness for Information Management (IM) Practitioners* provide detailed information on the development of strategies to support all departmental staff.

4.8 Review and Update

Review and update the governance framework, accountability and organizational structures to accommodate significant changes that impact departmental operations. At a minimum, schedule a formal review every 2 years. Identify areas of the IM program that are not operating effectively and may require a modification in staffing allocation. Significant events that change the scope or nature of the department's business may also impact the governance and organizational structure. Review and update may be required in the event of:

- New legislation or new lines of business

Guideline – Information Management (IM) Governance, Accountability and Organization

- Reorganization of the Department

5.0 Glossary

[Information Management](#)

[TRIM](#)

5.1 Acronyms

GNL	Government of Newfoundland and Labrador
IM	Information Management
IMCAT	Information Management Capacity Assessment Tool
OCIO	Office of the Chief Information Officer
ATIPP	Access to Information and Protection of Privacy
EDRMS	Electronic Document Records Management System
IT	Information Technology
RRDS	Records Retention and Disposal Schedule

6.0 References

[Management of Information Act](#)

[Information Management and Protection Policy, TBM 2009-335](#)

[Strategic Human Resource Management Division, Public Service Secretariat](#)

Guideline – Education and Awareness for Information Management (IM) Practitioners

Guideline – Information Management (IM) Education and Awareness for Government Employees

Guideline – Information Management (IM) Legal and Regulatory Framework

Guideline – Information Management (IM) Performance Measurement

Guideline – Information Management (IM) Vision, Mission and Guiding Principles

Guideline – Information Protection

7.0 Revision History

Date Reviewed	Reviewed By
2011-03-29	Iris Power, Director, Information Management Services
2011-04-05	Shelley Smith, Executive Director, Information Management
2011-04-07	Information Management Standards Board (IMSB)
2011-04-14	Government Records Committee (GRC)
2015-03-26	Bun Power, IM Consultant, IM Services

Appendix A: Sample Information Management (IM) Roles and Responsibilities



Sample
Accountability Model



Office of the Chief Information Officer

Guideline

Information Management Vision, Mission and Guiding Principles

Governance

Authority: Office of the Chief Information Officer

Audience: Information Management professionals and other resources responsible for the implementation and operation of a records and information management system (also referred to as an Information Management Program) within a department or other public body, as defined in the Management of Information Act.

Compliance Level: Recommended

Issuing Public Body: Office of the Chief Information Officer
Application and Information Management Services
Information Management Services

Original Issue Date: 2011 06 15

Date Last Reviewed: 2019 02 19

OCIO Reference: DOC03312/2011

Version Number: 3.0

Notice:

The Office of the Chief Information Officer (OCIO) is mindful of creating and delivering accessible materials, in line with the Government of Newfoundland and Labrador's Accessible Communications Policy. New materials created by OCIO align with policy requirements and modifications to existing materials will occur as part of the standard review cycle.

This document is available in alternate format. Please contact OCIO@gov.nl.ca.

Forward questions and/or comments related to this document to IM@gov.nl.ca.

Table of Contents

1.0 Overview	4
2.0 Purpose	5
3.0 Definitions and Acronyms	6
4.0 Recommended Approach	8
4.1 IM Vision Statement.....	8
4.2 IM Mission Statement.....	9
4.3 IM Guiding Principles	9
5.0 Roles and Responsibilities	11
6.0 Supporting Materials and Version History	12
Appendices	13

1.0 Overview

The Information Management (IM) Vision, Mission and Guiding Principles Guideline (hereafter referred to as the Guideline) is designed to assist departments and other public bodies in the Government of Newfoundland and Labrador to develop an appropriate IM Vision, Mission and Guiding Principles that will serve to drive the design, development, implementation and management of an effective IM Program.

Departments and other public bodies may find that the IM Vision, Mission and Guiding Principles as set out in this Guideline are adequate for their purposes, or they may wish to develop their own using the model contained in this Guideline.

Guidelines are recommended actions, general approaches and operational behaviors. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies, directives and standards.

Guidelines issued by OCIO recommend actions and are not compulsory, as they take into consideration the varying nature of information management programs.

2.0 Purpose

The IM Vision, Mission and Guiding Principles Guideline provides a recommended approach that will serve to drive the design, development, implementation and management of an effective IM Program. This Guideline is part of a broader GuideBook that supports the requirement set forth in Management of Information Act (MOIA) for permanent heads of departments and other public bodies to implement a records and information management system.

Expected Deliverable(s)

1. An approved and published document, available to all staff of the organization that contains the IM Vision Statement, the IM Mission Statement and the IM Guiding Principles; this can be a standalone document or ideally, a section contained within the IM Program Plan.

The GuideBook, also known as the Guide to IM for Public Bodies, includes the following guidelines.

1.0 Foundation

- 1.1 IM Governance, Accountability and Organization
- **1.2 IM Vision, Mission and Guiding Principles**
- 1.3 IM Legal and Regulatory Framework
- 1.4 IM Program Plan

2.0 Components

- 2.1 IM Policy Instruments
- 2.2 IM Performance Measurement
- 2.3 Service Continuity
- 2.4 Education and Awareness for IM Professionals
- 2.5 IM Education and Awareness for Employees
- 2.6 Physical Records Storage Development and Use
- 2.7 Information Protection

3.0 Tools

- 3.1 Records and Information Inventory
- 3.2 Classification Plan Development for Operational Records
- 3.3 Records Classification Plan Implementation
- 3.4 Disposal of Records
- 3.5 Record Imaging Services

3.0 Definitions and Acronyms

A complete listing of terms are located on the OCIO website - Information Management and Protection (IM&P) Glossary of Terms.

Vision - A vision defines the desired or intended future state of an organization or program in terms of its fundamental objective and/or strategic direction. Vision is a long-term view, describing how the organization or program would like to be and what it would look like.

Vision Statement - A vision statement outlines what the organization wants to be. It concentrates on the future, is a source of inspiration and provides clear focus.

IM Vision Statement - An IM vision statement is the inspiration and framework for IM strategic planning and IM Program development. Features of an effective IM vision statement include a description of a desired state for IM that features clear wording, lack of ambiguity, realistic aspirations and alignment with organizational values and culture.

Mission - A mission is a brief measurable long-term outcome statement, which defines where an organization is going and why.

Mission Statement - A mission statement is a formal, short, written statement of the purpose of a company or organization. The mission statement should guide the actions of the organization, spell out its overall goal, provide a sense of direction, and guide decision-making. It provides “the framework or context within which the company’s strategies are formulated.”

IM Mission Statement - An IM mission statement is a concise, formal statement of the purpose of the IM Program within an organization. It should indicate how the Information Management programs and services will enable the mandate of a public body and support its compliance requirements.

Principle - A principle is a statement of fundamental value, a rule, or belief tied to business objectives and requirements, and establishes constraints on the manner in which business is conducted.

Guiding Principles - Guiding principles articulate the fundamental values that provide overall program direction throughout its operation irrespective of changes in its goals, requirements or resources.

Guideline – Information Management Vision, Mission and Guiding Principles

IM Guiding Principles - IM Guiding Principles are used to help formulate the initial IM Program and IM Governance model, as well as to provide a framework for decision making.

The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
IM	Information Management
MOIA	Management of Information Act
OCIO	Office of the Chief Information Officer
CGSB	Canadian General Standards Board
ISO	International Standards Board

4.0 Recommended Approach

The intent of this Guideline is to provide recommended actions, general approaches and operational behaviors that when implemented will serve to drive the design, development, implementation and management of an effective IM Program

4.1 IM Vision Statement

IM Vision Statement Example:

[Public body] will sustain a professional Information Management program to enable its mandate, facilitate legislative and policy compliance, appropriately protect information, and support services to citizens.

The attainment of the IM Vision contributes to the following outcomes:

- Staff and stakeholders have easy, efficient and managed access to the information that they need to do their jobs and meet legal/regulatory requirements;
- Programs have quality information to support their mandate and for the delivery of services to stakeholders;
- A public body has information to document and trace decisions and processes;
- Information is safeguarded and made available as appropriate;
- The exchange of information within the public body and between the public, stakeholders and other government entities will be easily accomplished and reliable;
- Increased quality of management and program decision-making and service delivery;
- Increased confidence in the privacy and security of information entrusted to or generated by the public body.

4.2 IM Mission Statement

IM Mission Statement Example:

In the [Public body], the mission of IM is:

To deliver efficient and effective Information Management programs and services to enable the mandate of [Public body] and support its compliance requirements.

4.3 IM Guiding Principles

IM Guiding Principles are used to help formulate the initial IM Program and IM Governance model, as well as to provide a framework for decision making. They are used to:

- Provide a clear linkage to mandate and business priorities;
- Guide the IM organization in the development and delivery of the IM Program;
- Facilitate communication of IM services and initiatives to users; and
- Help to simplify IM decision-making process.

A public body should establish the IM Guiding Principles that will guide the development and implementation of its IM Program and Plan. The OCIO is guided by the relevant International Standards Organization (ISO) and Canadian General Standards Board (CGSB) standards for its policy development framework and overall approach. The development of Information Management and Protection policies, directives, standards and guidelines by the OCIO is based upon the following principles, which may be adopted by public bodies, or modified to suit their individual requirements:

IM Guiding Principles Example:

- Promoting records creation to support the conduct of business, comply with the regulatory environment and provide necessary accountability.
- Enabling transparency of decision-making and expenditure through the development of proper information management and protection practices throughout Government operations and systems, and the appropriate training of information management personnel to provide effective service delivery.

Guideline – Information Management Vision, Mission and Guiding Principles

- Enabling legislative compliance where a requirement to retain records is articulated or where legislative compliance relies upon timely and appropriate access to information resources.
- Lifecycle management of all information in all formats during all lifecycle stages from creation (through use and management) to disposal (through destruction, deletion or transfer to The Rooms Provincial Archives Division for permanent preservation).
- Providing information authenticity, integrity and security to protect information holdings from loss, inappropriate access or use, disclosure, alteration, removal or destruction; thereby ensuring confidentiality, integrity, availability and accountability over time.
- Risk management through the assurance that security risks are identified, acceptable and that control mechanisms are in place.

5.0 Roles and Responsibilities

Departments and other public bodies

Under MOIA, departments and other public bodies must develop a records and information management system. The GuideBook and supporting materials assist a department or other public body in the development of a records and information management system, often referred to as an IM Program. Compliance with MOIA, OCIO's IM&P Policy approved by Treasury Board and subsequent policies, directives and standards that the OCIO develops is mandatory.

Directors responsible for IM

Directors responsible for IM within a department or other public body should develop and publish vision statement, mission statement and guiding principles for information management to support the overall IM Program and Plan.

Office of the Chief Information Officer

As part of OCIO's mandate, the OCIO

- defines, develops and publishes IM&P policy instruments as needed;
- is responsible for IM&P policy instrument lifecycle management;
- implements appropriate communications regarding IM&P policy instruments; and
- manages, maintains and monitors IM&P policy instruments for effectiveness and compliance.

6.0 Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published internet location.

Management of Information Act

<http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)

https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.html

OCIO Website

<https://www.ocio.gov.nl.ca>

Information Management and Protection (IM&P) Glossary of Terms

<http://www.ocio.gov.nl.ca/ocio/im/glossary.html>

Guide to IM for Public Bodies

<https://www.ocio.gov.nl.ca/ocio/im/practitioners/chart.html>

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2011-06-15	Version 1
2017-05-23	Version 2
2019-02-19	Version 3

Appendices

A listing of policy instruments, support materials including templates and examples are available on the OCIO website to guide departments and other public bodies in the development of standard documents and content, supporting IM program development and management and the growth of IM capacity.

Appendices listed below directly relate to the GuideBook: IM Vision, Mission and Guiding Principles and are published independent of this Guideline on the OCIO website, <https://www.ocio.gov.nl.ca/ocio/im/practitioners/chart.html>.

Appendix	Title
A	IM Vision, Mission and Guiding Principles Guideline – Checklist
B	Quick Reference – Records and Information Management System
C	IM Vision, Mission and Guiding Principles – Template and Example

Other GuideBook References:

IM Program Plan Guideline



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – INFORMATION MANAGEMENT (IM) LEGAL AND REGULATORY FRAMEWORK

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015 04 01
OCIO TRIM Number	DOC03310/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	
Related Guidelines	

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	3
2.0	Scope	3
3.0	Recommended Approach.....	3
3.1	Introduction.....	3
3.2	How It Works:	4
3.3	Identifying IM Legal and Regulatory Requirements	5
3.4	IM Legal and Regulatory Framework	5
4.0	Glossary	7
4.1	Definitions.....	7
4.2	Acronyms.....	7
5.0	References.....	7
6.0	Revision History	7

GUIDELINE FOR IM LEGAL AND REGULATORY FRAMEWORK

1.0 Overview

This guideline assists public bodies in developing an effective Information Management (IM) Legal and Regulatory Framework. An IM Legal and Regulatory Framework is a compilation of all of the legislation, policy, regulations and agreements that contain IM requirements with which the public body must demonstrate compliance. Having an effective IM Legal and Regulatory Framework will serve to:

- Align and integrate all IM Compliance requirements and responsibilities into a single IM Legal and Regulatory Framework;
- Assign roles, responsibilities and accountabilities for each IM Compliance requirement listed in the IM Legal and Regulatory Framework;
- Satisfy IM Compliance requirements listed in the IM Legal and Regulatory Framework, and improve organizational efficiency in doing so, making the most efficient and effective use of resources and activities;
- Improve the ability to communicate the level of IM Compliance and organizational commitment to IM Compliance;
- Protect the reputation, interests of and confidence in the organization.

2.0 Scope

This Guideline applies to or may be used by all public bodies (hereafter referred to as departments), as defined in the [Management of Information Act](#). The audience for this guideline includes all individuals responsible for the operation of an IM program within their department.

3.0 Recommended Approach

3.1 Introduction

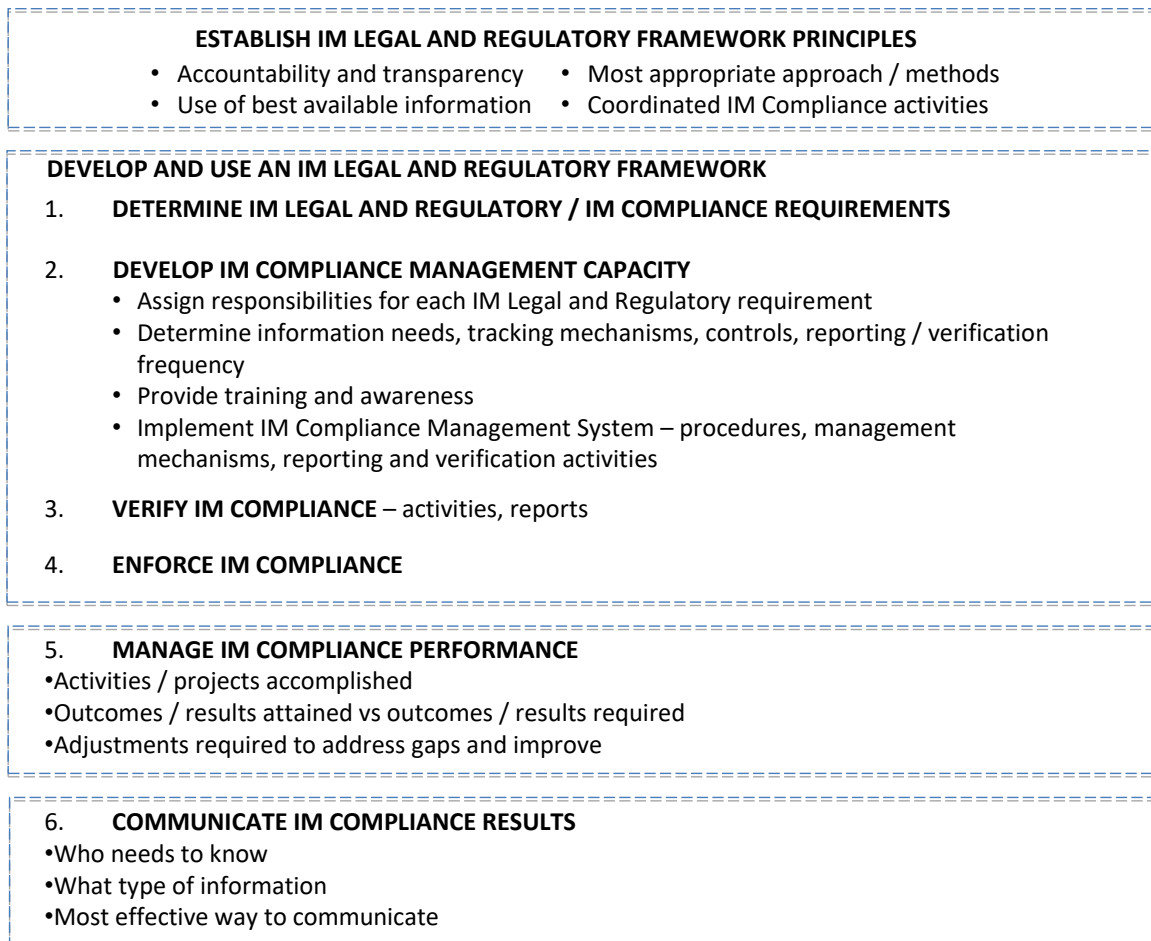
An IM Legal and Regulatory Framework incorporates all of the IM compliance requirements that a department must satisfy. The department needs to be able to:

- Determine the IM legal and regulatory requirements that apply to it, are binding on it and / or with which it must comply;
- Develop its IM Legal and Regulatory Framework to encompass IM legal and regulatory requirements, including IM compliance requirements;
- Identify by position title or role who is assigned responsibility for each IM compliance requirement listed in the IM Legal and Regulatory Framework;
- Promote IM compliance through training and awareness activities;

- Enforce IM compliance by verifying the extent of IM compliance with the IM Legal and Regulatory Framework, and identifying any areas of non-compliance;
- Address any non-compliance issues; and
- Report on the satisfaction of all IM compliance responsibilities and accountabilities listed in the IM Legal and Regulatory Framework.

3.2 How It Works:

The process of managing IM Compliance using an IM Legal and Regulatory Framework is shown in the diagram below:



3.3 Identifying IM Legal and Regulatory Requirements

Within the Government of Newfoundland and Labrador, IM legal and regulatory Requirements are found in the following sources:

- *Management of Information Act*
- *Access to Information and Protection of Privacy Act*
- *Electronic Commerce Act*
- *The Rooms Act*
- *Transparency and Accountability Act*
- *Evidence Act*
- *Financial Administration Act*

Other applicable IM compliance requirements that are binding on or impose duties and responsibilities on the Government of Newfoundland and Labrador with respect to information, its management and its protection may be found in:

- Federal and Provincial legislation and regulations where applicable for specific departments;
- Government of Newfoundland and Labrador policy, procedures, standards and guidelines;
- Departmental contractual requirements agreements and other similar undertakings.

Once an inventory of IM legal and regulatory requirements has been developed and incorporated in an IM Legal and Regulatory Framework, the department's legal advisor should review the list for accuracy, relevance and completeness.

3.4 IM Legal and Regulatory Framework

The IM Legal and Regulatory Framework is typically represented as a table or matrix:

- This matrix shows the complete list of IM legal and regulatory requirements; and
- These IM legal and regulatory requirements are mapped against the department management team role or roles to which responsibility for satisfying the IM compliance requirement is assigned.

It is developed as a simple matrix, listing:

- In the first column of the table or matrix, all IM legal and regulatory requirements;
- In the second column, the oversight entities for each IM legal and regulatory requirement; and
- In subsequent columns, show the position(s) or roles within the public body who are specifically responsible for each IM legal and regulatory requirement.

It is usually constructed as a table that is from one to three pages in length. An illustrative IM Legal and Regulatory Framework matrix is shown below:

ILLUSTRATIVE IM LEGAL AND REGULATORY FRAMEWORK

IM LEGAL / REGULATORY / COMPLIANCE REQUIREMENT	DM	DIRECTOR IM	ATIPP COORDINATOR	DIRECTOR FINANCE AND GENERAL OPERATIONS	ADM / DIRECTOR "A"	ADM / DIRECTOR "B"
1. Management of Information Act		X				
2. Access to Information and Protection of Privacy Act			X			
3. Electronic Commerce Act				X		
4. Rooms Act		X				
5. Transparency and Accountability Act	X					
6. Evidence Act						
7. Financial Administration Act				X		
8. Federal / Provincial Legislation					X	
9. Federal / Provincial Regulations						X
10. GNL Policies, Procedures, Standards, Guidelines		X	X	X	X	X
11. Contractual Requirements and Agreements				X	X	

Notes:

- In an IM Legal and Regulatory Framework, it is typical to specify the reporting chain from the individual / role responsible for the specific compliance requirement up to the head of the organization.
- In its IM Legal and Regulatory Framework matrix, a department should identify the role responsible for each IM legal and regulatory requirement; and
- Sometimes this chain of responsibility up to the head of the public body may be specified in job descriptions and in other cases the required relationship may be defined in a directive, letter or memorandum that assigns responsibility for one or more IM legal and regulatory requirements to a specific position, role or person.

4.0 Glossary

4.1 Definitions

[Information Management](#)

4.2 Acronyms

IM	Information Management
----	------------------------

5.0 References

Management of Information Act

Access to Information and Protection of Privacy Act

Electronic Commerce Act

The Rooms Act

Transparency and Accountability Act

Evidence Act

Financial Administration Act

Information Management and Protection Policy, TBM 2009-335

6.0 Revision History

Date Reviewed	Reviewed By
2010-12-22	Iris Power, Director of Information Management Services
2011-02-04	Shelley Smith, Executive Director Information Management
2011-02-14	Information Management Standards Board (IMSB)
2011-03-04	Government Records Committee (GRC)
2015-04-01	Bun Power, IM Consultant, IM Services



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – INFORMATION MANAGEMENT (IM) PROGRAM PLAN

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015 04 01
OCIO TRIM Number	DOC04592/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	
Related Guidelines	See References

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

- 1.0 Overview3
- 2.0 Scope.....3
- 3.0 Background.....3
- 4.0 Recommended Approach.....4
 - 4.1 Review IM Drivers and Requirements:.....5
 - 4.2 Identify Business Alignment Requirements.....5
 - 4.3 Perform Current State Assessment.....6
 - 4.4 Set Goals and Objectives.....6
 - 4.5 Identify Services6
 - 4.6 Define Service Management Processes8
 - 4.7 Plan Education and Awareness8
 - 4.8 Define Resource Requirements and Allocation9
 - 4.9 Establish Governance and Organization.....9
 - 4.10 Establish Program Management Framework.....9
 - 4.11 Identify Performance Management and Reporting Requirements..... 10
 - 4.12 Obtain Program Plan Approval..... 10
- 5.0 Glossary.....10
 - 5.1 Acronyms..... 10
- 6.0 References..... 11
- 7.0 Revision History 11
- Appendix A: Sample Information Management (IM) Goals and Objectives Tracking Table 12
- Appendix B: OCIO Information Management Branch Service Catalog..... 13

INFORMATION MANAGEMENT (IM) PROGRAM PLAN

GUIDELINE

1.0 Overview

An Information Management (IM) Program Plan outlines how IM works in a department. This includes governance, organization, management, services, performance management and reporting. This guideline is designed to assist public bodies in the Government of Newfoundland and Labrador to develop an appropriate Information Management (IM) Program Plan that will serve to drive the design, implementation, operation and management of an effective IM Program.

2.0 Scope

This Guideline applies to or may be used by all public bodies (hereafter referred to as departments), as defined in the *Management of Information Act*. The audience for this guideline includes all individuals responsible for the operation of an IM program within their department.

3.0 Background

The IM Program Plan brings to life how the IM capabilities and services are created, delivered and managed. It is a blueprint for IM within the department and a very useful guide for the typical employee in fulfilling their job responsibilities. Put simply, the IM Program Plan has an operational perspective and describes:

- What IM services, projects, activities and events are provided to whom, when and why;
- How they are provided or delivered, and by whom; and
- How they are planned and managed to ensure end user and management satisfaction.

Implementing an IM Program Plan will contribute to the following desired outcomes:

- Increased quality of IM Program planning, service delivery, management and related decision-making;
- Increased confidence that the department is implementing a reasonable IM Program, including policies, services, procedures, standards and guidelines in accordance with requirements of the *Management of Information Act* and the Information Management and Protection Policy;
- Better-managed, aligned and mission-enabling IM services;
- Greater relevance and effectiveness of IM through the implementation of the IM Program Plan;
- Better collaboration and coordination among the IM organization, its IM service delivery partners, the end user community and other stakeholders; and
- Increased confidence that IM stakeholders' requirements are being satisfied.

4.0 Recommended Approach

IM Program planning follows a similar process to business and strategic planning, but is entirely focused on the development and delivery of an IM Program that supports the business mission and business operations of the department. The approach described in this document can be tailored by the department as required to meet its unique mandate and lines of business. This process consists of the following activities:

- Review IM Drivers and Requirements - Identify what is driving IM including the business, legal, regulatory and other compliance requirements;
- Identify Business Alignment Requirements - Identify how the IM Program must align with internal and external linkages;
- Perform Current State Assessment - Examine how IM is currently functioning within the department, in other similar organizations and what various external IM public bodies and standards setting bodies are doing in IM. Identify any gaps, deficiencies, lessons learned elsewhere and opportunities for improvement;
- Set Goals and Objectives - Set goals, objectives and priorities for IM for the planning period to lay out what IM must do to support the business strategy and business operations of the department;
- Identify Services – Identify what IM services will be provided to whom, when, where including externally supplied and internal services. Consider also what IM projects and other IM activities and events will be undertaken as part of the IM Program;
- Define Service Management Processes – Outline how services will be delivered as a part of the program;
- Plan Education and Awareness – What training and awareness activities and events will be undertaken;
- Define Resource Requirements – What resources will be required to deliver the IM Program, including people, funding and facilities;
- Establish Governance and Organization – Explain the structure of IM in the department and how it will be governed;
- Establish IM Program Management Framework – How will the IM Program be managed and delivered, including resource allocation and management and IM Service Delivery;
- Identify Performance Measurement and Reporting Requirements – IM Performance Measurement and Reporting requirements track how the program is progressing according to the plan;
- Obtain Program Plan Approval – Once completed, the IM Program Plan is presented to the Executive for consideration and approval.

The following sections include detailed descriptions of what needs to be done at each step in the IM Program planning process.

4.1 Review IM Drivers and Requirements:

IM Drivers and Requirements identify what is driving IM including the business, legal, regulatory and other compliance requirements. Completing this step will enable those developing the IM plan to know what it is that the business intends to do and how IM can best support the business strategy and operations with the right IM services.

This is usually done by reviewing the following sources of information:

- Business Strategy – Since IM must support the business operations of the department, IM needs to understand the business strategy and objectives as set out in the department's business plan. Ideally, the business plan should contain direction from Senior Management on policy, plans, priorities, objectives, desired outcomes, and may also include specific direction or objectives for IM;
- IM Vision and Guiding Principles – Defines the strategic direction and guidance for IM. The guideline *Information Management (IM) Vision, Mission and Guiding Principles* details how to establish these foundational components of the IM Program;
- Business Requirements – what IM requirements need to be fulfilled and what IM services do the various stakeholders require;
- IM Legal and Regulatory Framework – review all of the IM Legal and Regulatory requirements, including all IM Compliance requirements and how the IM Legal and Regulatory Framework and other IM compliance requirements are to be managed. The guideline *Information Management (IM) Legal and Regulatory Framework* outlines how to establish this at a departmental level.

4.2 Identify Business Alignment Requirements

IM needs to be aligned within the department and with external suppliers and stakeholders in order to best support the department. This is usually done by aligning and harmonizing the IM Program Plan with the department's strategic / business plan, strategic HR plan, Business Continuity Plan and other similar plans and undertakings such that IM is part of the essential business fabric of the department and supports the department's mission.

Good practice would be to develop the IM Program Plan in parallel with the department's business plan to ensure alignment and synchronization of objectives and services. In this approach, the department would follow this process:

- First, the business planners publish business planning guidance including the business planning process and schedule for all elements of the department;
- Second, the Executive or Senior Management may also provide specific IM guidance that must be considered in the development of the IM Program Plan;
- Third, IM and the other business areas of the department coordinate their planning activities such that the business requirements are known to IM and such that IM can plan to support the business requirements;
- Fourth, the Executive or Senior Management would review and approve the IM Program Plan before it is reviewed and integrated as part of the department's business planning process; and
- Fifth, the department's business planners would review business plans and the IM Program Plan to ensure adequate alignment and synchronization.

4.3 Perform Current State Assessment

Departments that have recently completed an assessment using the Information Management Capacity Assessment Tool (IMCAT) will have identified:

- How IM is currently functioning within the department and in other similar organizations;
- Various external IM bodies and standards setting bodies are doing in IM; and
- Gaps, deficiencies, lessons learned elsewhere and opportunities for improvement.

The findings summarized in the IMCAT report may need to be updated to reflect changes that have occurred since its completion or any department specific requirements. This information will be used to support the requirements described in subsequent sections.

4.4 Set Goals and Objectives

The IM Program Plan must define the goals and objectives for IM within the department and explain how these will be attained. It will describe how the business requirements, IM legal and regulatory requirements and the business operations of the department will be supported through the provision of IM services and the completion of IM projects and activities.

This approach will enable the IM Program planner to map IM objectives to each specific IM driver or business requirement, to explain what are the measures and indicators to evaluate the achievement of that objective, and to define what services and resources are required for IM to attain that objective. A sample “IM Goals and Objectives Tracking Table” is included in Appendix A.

4.5 Identify Services

The IM Program Plan must identify the IM services that are available externally and internally. This can be thought of as the IM service catalogue for the department, and would serve as a useful reference for staff at all levels.

4.5.1 Internal Services

The IM Program Plan should describe the IM services that are provided by the department, including those supplied by its IM organization and any other IM services that are provided from other parts of the department. The IM Program Plan should provide the following information:

- IM Service Description - Describe each internal IM service, as provided by the supplier of that service (normally the IM organization);
- IM Service Provisioning - Identify who provides the IM service, the IM service manager and any conditions of use;
- IM Service Management – Identify who in the department’s IM organization is the point of contact for that service, how service management will work, and how problems or issues will be handled and managed;

The “OCIO Information Management Branch Service Catalog”, included in Appendix B, provides an example of the type of information, level of detail, etc that should be included. Examples of internal IM services include:

- IM Advisory Services – advice and guidance on IM Policy, procedures, standards and guidelines;
- Electronic Documents and Records Management System - TRIM management and scanning of paper-based documents
- Records Management
 - Classification System
 - Records Retention and Disposal Schedule development and management
 - Collections management – records rooms, storage containers, shelving
 - Libraries – publication collections
- IM Facilities – file and records rooms, mail distribution system,
- Storage – physical and electronic
- Information Protection / Information Security Management – services related to the protection and security of information assets created, used and managed by the department. This should address the four component parts of Security:
 - Information Security – the policies and procedures based on sensitivity and confidentiality for the creation, handling, use, storage, conveyance and disposition of information, including:
 - Security / Sensitivity System – criteria for determining what constitutes a confidential or sensitive record;
 - Access Controls and Access Management – control of the assignment of access permissions to individuals such that they may access sensitive or confidential information held in physical and / or electronic records;
 - Vital Records - Vital records are “records that are vital to the continuing functioning of the organization.” These records are essential for preserving, continuing or reconstructing the operations of a department and protecting the rights of the organization, its employees and its stakeholders;
 - Access to Information Requests – a service governed by the *Access to Information and Protection of Privacy Act* (ATIPPA) that provides access to, but also specific protections for, government records (including personal information) in the custody and control of a department;
 - Physical Security – of facilities (offices, rooms and work areas) and storage containers used to store information (such as filing cabinets and lockable compartments in work stations);
 - Personnel Security – may include background checking of selected employees who handle certain sensitive and / or confidential information

4.5.2 External Services

External services fall into two categories. These are services provided by the OCIO and services provided by third party vendors. The IM Program Plan should describe the externally supplied IM services that the department will use, explaining:

- IM Service Description and Specifications – Provided for each external IM service, as provided by the supplier of that service;

- Basis - Under what contract, arrangement or agreement is the IM service being provided, including conditions of use;
- IM Service Provisioning - Identify who provides the IM service, the IM service manager and any conditions of use; and
- IM Service Management – Identify who in the department’s IM organization is the point of contact for that service, how service management will work, and how problems or issues will be handled and managed, and how the contract / agreement itself will be managed.

The OCIO supplies core IM and Information Technology (IT) services to government departments. See the “OCIO Information Management Branch Service Catalog” included in Appendix B for a detailed description of the services provided by the IM Branch, which focus on policies, standards and best practices for IM. Descriptions of IT services are available on the [OCIO Website](#). All services are provided and managed under the terms of the Service Level Agreement that exists between the OCIO and the department.

External IM Services are also be provided by third party vendors. In many cases, contracting for these external IM services is managed by central agencies (such as the OCIO or Government Purchasing Agency) through Master Standing Agreements. All departments are able to access IM services under such agreements. Examples include:

- Offsite Storage – for records, backup media and Vital Records;
- Physical Destruction – such as shredding services.

Contact your manager of financial operations to access master standing offer agreements related to IM.

4.6 Define Service Management Processes

The IM Program Plan must define how IM services will be managed within the department. IM Service Management should define for each service:

- Service Description – see above;
- Roles and Responsibilities - in service delivery and management
- Service Standards – including for example availability of services
- Service Management / Service Level Management – how changes, problems and issues are managed; and
- Service Continuity Management – to what extent and how the IM service will respond to disruptive events and to what extent service continuity will be provided during a disruptive event. The IM Service Continuity Plan must be closely aligned with the department’s Business Continuity Plan and must describe the arrangements that will be enacted to provide for a required and continuing level of IM service that supports business needs during a disruptive event.

4.7 Plan Education and Awareness

The IM Program Plan must contain an IM education and awareness component to accommodate the needs of both departmental employees and IM practitioners. Education and awareness must be recognized as an important component of the IM program. Without education and awareness:

- Employees may not understand their IM responsibilities as public employees
- IM practices may be inconsistent across the department
- Employees may not be aware of new policies, standards and guidelines related to IM

The following guidelines are used to develop departmental IM Education and Awareness Plans:

- “Information Management (IM) Education and Awareness for Government Employees”
- “Education and Awareness for Information Management (IM) Practitioners”

4.8 Define Resource Requirements and Allocation

The IM Program Plan should present the resource requirements necessary to deliver the program, including:

- Funding - requirements for all costs for internal and external IM services, operating costs, personnel costs, and other costs for facilities, equipment and supplies;
- Human Resources - Requirements for the numbers and types of staff, including:
 - Salary; and
 - Training and development costs;
- Facilities – the facilities and space required, including any fit up costs for shelving, physical security and environmental controls (for paper based records).

These resource requirements should be developed and presented in the format required by the business planning process for ease of integration with other budgets and cost projections.

4.9 Establish Governance and Organization

The IM Program Plan should describe the IM Governance and Organization model, Development of this model is described in the Guideline *Information Management (IM) Governance, Accountability and Organization*. For the purpose of the plan, this information can be summarized and updated as required.

4.10 Establish Program Management Framework

The IM Program Management Framework should describe how IM is managed within the department. It should explain:

- IM Program Management – how the management of the IM Program Plan and its various components, including IM services, projects, activities, events, training, professional development, career planning, performance appraisal and other undertakings are managed, such as:
 - A regular recurring IM organization management team meeting to review IM Program results, performance, status, issues and problems;
 - Regular reporting of IM Program results to senior management.

- Resource Management, including human resources, funding and facilities – how budgets are planned, approved, and managed
- Coordination Mechanisms – how the management and delivery of the IM Program will be coordinated within the department. These mechanisms are usually found in the planning process, in governance mechanisms, in recurring department management meetings where the IM director or manager will participate, and in special task teams formed to address a specific problem.

4.11 Identify Performance Measurement and Reporting Requirements

The IM Program Plan must include performance measurement and reporting requirements to track how the program is progressing according to the plan. This includes what gets reported, how it gets reported, and to whom it gets reported, including to senior management, the Executive, IM management, the end user community and other stakeholders. The Guideline *Information Management (IM) Performance Measurement* outlines how to develop IM performance management and reporting requirements.

4.12 Obtain Program Plan Approval

The IM Program plan must be reviewed as appropriate by departmental stakeholders as per established departmental protocols. The final IM Program Plan must be approved by the Executive.

5.0 Glossary

[Information Management](#)

[IM Vision](#)

[TRIM](#)

5.1 Acronyms

ATIPPA	Access to Information and Protection of Privacy Act
GNL	Government of Newfoundland and Labrador
IM	Information Management
IMCAT	Information Management Capacity Assessment Tool
OCIO	Office of the Chief Information Officer

6.0 References

[Management of Information Act](#)

Information Management and Protection Policy, TBM 2009-335

Guideline – Education and Awareness for Information Management (IM) Practitioners

Guideline – Information Management (IM) Education and Awareness for Government Employees

Guideline – Information Management (IM) Governance, Accountability and Organization

Guideline – Information Management (IM) Legal and Regulatory Framework

Guideline – Information Management (IM) Performance Measurement

Guideline – Information Management (IM) Vision, Mission and Guiding Principles

7.0 Revision History

Date Reviewed	Reviewed By
2011-01-19	Iris Power, Director of Information Services
2011-03-08	Shelley Smith, Executive Director Information Management
2011-03-17	Information Management Standards Board (IMSB)
2011-04-04	Government Records Committee (GRC)
2015-04-01	Bun Power, IM Consultant, IM Services

Appendix A: Sample Information Management (IM) Goals and Objectives Tracking Table



S:\Information
Management\IMCAsa

Appendix B: OCIO Information Management Branch Service Catalog



S:\Information
Management\IMCAT I



2. IM Program Components

2.1. Information Management Policy Instruments	29
2.2. Information Management Performance Measurement	30
2.3. Education and Awareness for IM Practitioners	31
2.4. IM Education and Awareness for Government Employees	32
2.5. Physical Records Storage and Development and Use	33
2.6. Information Protection	34



Office of the Chief Information Officer

Guideline

Information Management Policy Instruments

Governance

Authority: Office of the Chief Information Officer

Audience: Information Management professionals and other resources responsible for the implementation and operation of a records and information management system (also referred to as an Information Management Program) within a department or other public body, as defined in the Management of Information Act.

Compliance Level: Recommended

Issuing Public Body: Office of the Chief Information Officer
Application and Information Management Services
Information Management Services

Original Issue Date: 2011-05-21

Date Last Reviewed: 2019-04-04

OCIO Reference: DOC12091/2012

Version Number: 3.0

Notice:

The Office of the Chief Information Officer (OCIO) is mindful of creating and delivering accessible materials, in line with the Government of Newfoundland and Labrador's Accessible Communications Policy. New materials created by OCIO align with policy requirements and modifications to existing materials will occur as part of the standard review cycle.

This document is available in alternate format. Please contact OCIO@gov.nl.ca.

Forward questions and/or comments related to this document to IM@gov.nl.ca.

Table of Contents

1.0 Overview	4
2.0 Purpose	5
3.0 Definitions and Acronyms	6
4.0 Recommended Approach	8
4.1 Review Existing Policy Instruments	8
4.2 Identify or Define Policy Instruments.....	9
4.3 Identify or Define the Review and Approval Process	10
4.4 Create an IM Policy Instrument Inventory	11
4.5 Identify or Create Templates	12
4.6 Identify and Prioritize Requirements	12
4.7 Develop New or Update Existing Instruments.....	13
4.8 Review Cycle	13
4.9 Monitor and Verify	14
5.0 Roles and Responsibilities	15
6.0 Supporting Materials and Version History	16
Appendices	17

1.0 Overview

The Information Management (IM) Policy Instruments Guideline (hereafter referred to as the Guideline) is designed to assist departments and other public bodies in the Government of Newfoundland and Labrador to develop IM policy instruments and resultant framework that will serve to drive the design, development, implementation and management of an effective IM Program.

Developing IM policy instruments serve to strengthen a department or other public body's information management program and enable it to demonstrate compliance with legal, regulatory and operational requirements.

Guidelines are recommended actions, general approaches and operational behaviors. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies, directives and standards.

Guidelines issued by OCIO provide a recommended approach and are not compulsory, as they take into consideration the varying nature of information management programs.

2.0 Purpose

The IM Policy Instruments Guideline provides recommended actions, general approaches and operational behaviors to support the delivery of a managed inventory of IM policy instruments. This Guideline is part of a broader GuideBook that supports the requirement set forth in Management of Information Act (MOIA) for permanent heads of departments and other public bodies to implement a records and information management system.

Expected Deliverable(s)

An IM Policy Instrument Framework

1. An IM Policy Instrument Listing that highlights existing policy instruments and identifies those that may require development.
2. An IM Policy Instrument Inventory that lists all current elements as well as governance and lifecycle management requirements.
3. Policy instrument template and process requirements outlined by the business owner within the organization; supplemented to meet IM controls as required.

The GuideBook, also known as the Guide to IM for Public Bodies, includes the following guidelines.

1.0 Foundation

- 1.1 IM Governance, Accountability and Organization
- 1.2 IM Vision, Mission and Guiding Principles
- 1.3 IM Legal and Regulatory Framework
- 1.4 IM Program Plan

2.0 Components

- 2.1 IM Policy Instruments
- 2.2 IM Performance Measurement
- 2.3 Service Continuity
- 2.4 Education and Awareness for IM Professionals
- 2.5 IM Education and Awareness for Employees
- 2.6 Physical Records Storage Development and Use
- 2.7 Information Protection

3.0 Tools

- 3.1 Records and Information Inventory
- 3.2 Classification Plan Development for Operational Records
- 3.3 Records Classification Plan Implementation
- 3.4 Disposal of Records
- 3.5 Record Imaging Services

3.0 Definitions and Acronyms

A complete listing of terms are located on the OCIO website - Information Management and Protection (IM&P) Glossary of Terms.

IM Policy Instruments - IM policy instruments include policies, directives, standards, guidelines and procedures that provide direction or guidance on the management and protection of information aligned with the principles set forth in the Information Management and Protection Policy. OCIO extends the definition to include policy instrument supports such as Webpages, FYIs, FAQs, Quick Reference or Re-Use Materials as items to include in an IM policy instrument inventory.

Policy - Policies are high level, strategic statements, authorized by Senior Executive that dictate what type of position the organization has taken on specific issues. Compliance is mandatory. Example: Information Management and Protection Policy

Directive - Directives provide an official authoritative instruction or order to the organization supporting an existing policy. Compliance is mandatory. Example: Instant Messaging Directive

Standard - Standards are requirements that dictate uniform ways of operating and provide tactical blueprints for implementation of policies and directives. Compliance is mandatory. Example: Corporate Records Information Management Standard (CRIMS)

Guideline - Guidelines are recommended actions, general approaches and operational behaviors that allows some discretion or leeway in its interpretation, implementation, or use. Compliance is not mandatory but recommended. Example: Email Guideline

Procedure - Procedures are a fixed, step-by-step task level sequence of activities or course of action (with start and end points) that must be followed in the same order to correctly perform a task. Compliance is mandatory but exceptions may occur. Example: Business Process/Forms, such as the New Account Request Form

Information Management and Protection (IM&P) Policy - The IM&P Policy approved by Treasury Board provides authority for the OCIO to establish mandatory Information Management and Protection directives and standards for the Government of Newfoundland and Labrador and its public bodies. The IM&P Policy establishes the overall framework for IM&P within the Government of Newfoundland and Labrador and its public

Guideline – Information Management Policy Instruments

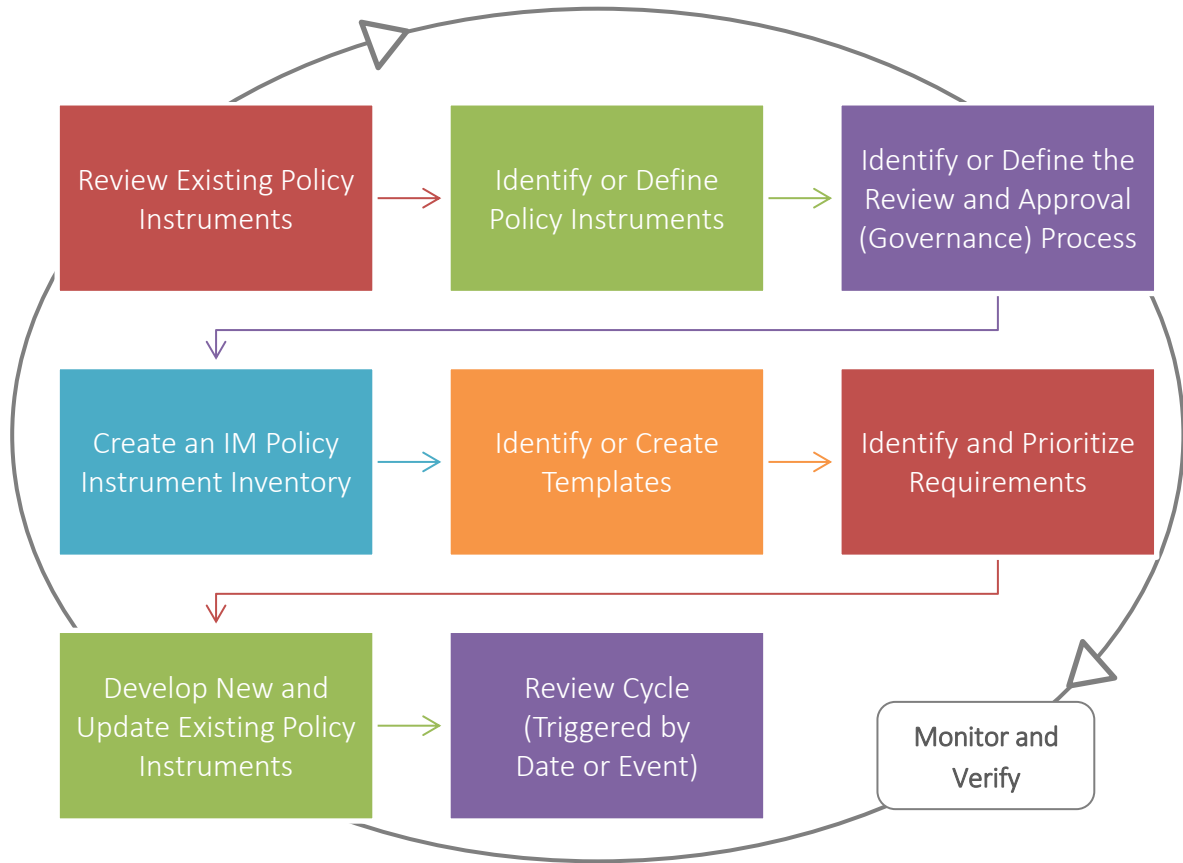
bodies in accordance with MOIA, ATIPPA, 2015, the Rooms Act and forms the basis for departments and other public bodies to develop their own supporting policy instruments aligned with the IM&P Principles.

The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
ATIPPA, 2015	Access to Information and Protection of Privacy Act, 2015
CRIMS	Corporate Records Information Management Standard
IM	Information Management
IM&P	Information Management and Protection
IMCAT	Information Management Capacity Assessment Tool
IMSAT	Information Management Self-Assessment Tool
IP	Information Protection
MOIA	Management of Information Act
OCIO	Office of the Chief Information Officer

4.0 Recommended Approach

The intent of this Guideline is to provide recommended actions that when implemented support the IM Program’s delivery of templated materials supported by an IM Policy Instrument Listing and managed through an IM Policy Instrument Inventory.



4.1 Review Existing Policy Instruments

A solid understanding of the existing materials is the first step in developing a set of organizational policy instruments. Create an IM Policy Instrument Listing that references materials that already exist either externally or internally. This listing will also minimize the likelihood that the department or other public body will duplicate effort in research and development of instruments that stakeholders, such as OCIO, may have already vetted and approved.

Consider the following when reviewing existing materials:

- OCIO’s website contains policies, directives, standards, guidelines as well as other supports, such as Webpages, FAQs, FYIs, Quick Reference and Re-Use materials for both public body employees and IM professionals;
- other IM Stakeholders such as Cabinet Secretariat and the ATIPP Office;
- internal policy instruments that provide IM direction;
- internal materials often in email message format that provide direction on IM topics; and
- the organization’s IM Legal and Regulatory Framework.

Note: Public bodies should reference OCIO policy instruments where possible and develop internal instruments only when necessary to support compliance with the direction stated within OCIO issued policy instruments.

4.2 Identify or Define Policy Instruments

Departments and other public bodies may already have in place templates and other requirements for policy instruments. Ensure to leverage existing processes and resources and only if necessary define and create new IM policy instruments and templates.

Departments and other public bodies are encouraged to establish consistent terminology related to policy instruments and accommodate any terminology; specific to the organization, that staff will recognize and know how to apply.

The generally accepted hierarchy of policy instruments is:

1. Policy
2. Directive
3. Standard
4. Guideline
5. Procedure

Defining and templating policy instruments as well as additional supports such as FAQs, FYIs, etc. can provide significant value to the department or other public body through increased organizational awareness and understanding. Create materials that provide

utility and accommodate various learning styles or communication channels and leverage opportunities such as IM month or Cybersecurity Awareness month to share existing information in new ways.

4.3 Identify or Define the Review and Approval Process

The review and approval process requires definition for each type of policy instrument. Identify the current process within the organization for the review and approval of policy instruments. IM policy instruments should be able to follow the same or very similar governance process. The creation of a new IM governance process should only occur if there is no process currently in place within the department or other public body.

Defining this governance process involves a variety of stakeholders and where possible should align with current governance processes, if they already exist, within the department or other public body.

Stakeholders that may be engaged in these processes include:

- the Senior Executive within the department or other public body should provide approval for selected type of instruments;
- the Executive responsible for IM within the department or other public body should provide approval for selected type of instruments;
- the legal counsel responsible for advice and guidance on IM-related issues including legislative and regulatory requirements for records retention and disposal;
- the department or other public body's Access to Information and Protection of Privacy (ATIPP) Coordinator;
- the divisional or program area management team;
- the Director or Executive responsible for policy development within the department or other public body; and
- the Director responsible for internal communications within the department or other public body.

Ensure that each of the stakeholders understand their role and responsibilities and document the information for future reference. Further information is located in OCIO's GuideBook: IM Governance, Accountability and Organization Guideline.

4.4 Create an IM Policy Instrument Inventory

There may already be IM policy instruments within the department or other public body. Gather the information and create an inventory of any existing IM policy instruments. The table below highlights recommended information to include in the inventory. A sample inventory is included in the IM Policy Instrument Inventory – Template and Example file found on the OCIO website.

Consider the below when creating an IM Policy Instrument Inventory.

- Classification and document references within HPRM, or other electronic content management system;
- Document controls such as managing versions;
- Tracking and managing the graphics and other inserted materials within the documents;
- Naming convention for internal documents but also website publishing standards;
- Maintaining the original issue date and documenting the last review date;
- Establishing an acceptable and consistent review cycle (based on capacity and likelihood of change); and
- Documenting other criteria, such as those noted below:
 - instrument type and compliance level
 - policy instrument owner
 - review status
 - published location & audience
 - topic/information tags
 - linkage to legal, regulatory or operational requirements.

4.5 Identify or Create Templates

Having templates for all policy instruments and support materials facilitates consistency. The content within a template serves as a checklist making it easier to prepare a policy instrument and that the required information is included. Be sure to consult internally within your department or other public body to verify whether there are existing template requirements for policy instruments.

Visit the OCIO website to view available templates and other re-use materials. The implementation of these re-use materials is not mandatory but provided as examples; modification to meet the needs of the organization will still be required.

4.6 Identify and Prioritize Requirements

Follow the steps below in identifying and prioritizing requirements:

1. Based on the IM Policy Instrument Inventory identify policy instruments that must be updated using the new templates.
2. Create a listing of IM policy instruments that are needed using the categories and gaps identified in the Inventory. Existing documentation, such as those itemized below, may provide a good basis for this listing:
 - a. IM assessment reports:
 - i. Information Management Capacity Assessment Tool (IMCAT);
 - ii. Information Management Self-Assessment Tool (IMSAT);
 - b. IM Legal and Regulatory Framework; and
 - c. IM Program Plan.
3. Reference the goals and objectives as identified in the department or other public body's IM Program Plan to prioritize this listing.
4. Assign resources to lead development, review and approval processes.

4.7 Develop New or Update Existing Instruments

As noted above departments and other public bodies should reference OCIO policy instruments where possible and develop internal instruments only when necessary to support compliance with the direction stated within OCIO issued policy instruments.

When developing policy instruments departments and other public bodies should:

- review available related types of work and ensure that the proposed instrument does not conflict with OCIO issued policies, directives or standards (e.g., Information Management & Protection Policy, Acceptable Use of the Government Network and IT Assets Directive, Instant Messaging Directive, etc.);
- consult with IM Advisory Services (OCIO) to verify whether OCIO has any existing information related to the area of development that can help guide the department or other public body;
- use the most current internal template to prepare draft policy instruments. This may mean transferring content that exists in a program area template or informal format to the approved template;
- follow a formal review and approval process;
- publish the policy instrument in a location and format accessible to **all** employees;
- communicate the policy instrument to **all** employees; and
- communicate the policy instrument to stakeholders.

Reference the OCIO's GuideBook: IM Education and Awareness for Employees Guideline to support the implementation, adoption and reinforcement of policy instruments.

4.8 Review Cycle

Assign responsibility for ensuring that IM policy instruments are reviewed and updated, as required, based on a regular schedule or triggering event; keeping the IM Policy Instrument Inventory updated will make this process easier. Reviewing policy instruments including supports ensures that content is valid, accurate and that any linkages on websites or intranets are working properly.

4.9 Monitor and Verify

A review and validation of program compliance, performance and capacity are the mechanisms for monitoring and verifying IM. IM policy instruments, templates and supports need to be lifecycle managed to ensure they are providing accurate and relevant information to the organization and assessed to validate that they continue to support IM performance and capacity development.

5.0 Roles and Responsibilities

Departments and other public bodies

Under MOIA, departments and other public bodies must develop a records and information management system. The GuideBook and supporting materials assist a department or other public body in the development of a records and information management system, often referred to as an IM Program. Compliance with MOIA, OCIO's IM&P Policy approved by Treasury Board and subsequent policies, directives and standards that the OCIO develops is mandatory.

Directors responsible for IM

In addition to promoting, the adoption of OCIO policy instruments through education and awareness, directors responsible for IM within a department or other public body should develop their own policy instruments and framework to support internal legal, regulatory and operational requirements. Such policy instruments must not contradict the policies, directives, and standards established by the OCIO under the authority of the IM&P Policy.

Office of the Chief Information Officer

As part of OCIO's mandate, the OCIO

- defines, develops and publishes IM&P policy instruments as needed;
- is responsible for IM&P policy instrument lifecycle management;
- implements appropriate communications regarding IM&P policy instruments; and
- manages, maintains and monitors IM&P policy instruments for effectiveness and compliance.

6.0 Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published internet location.

Management of Information Act

<http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)

https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.htm

Access to Information and Protection of Privacy Act, 2015

<http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm>

Rooms Act

<https://assembly.nl.ca/legislation/sr/statutes/r15-1.htm>

OCIO Website

<https://www.ocio.gov.nl.ca>

Information Management and Protection (IM&P) Glossary of Terms

<http://www.ocio.gov.nl.ca/ocio/im/glossary.html>

Guide to IM for Public Bodies

<https://www.ocio.gov.nl.ca/ocio/im/practitioners/chart.html>

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2011-05-20	Version 1
2015-03-31	Version 2
2019-04-04	Version 3

Appendices

A listing of policy instruments, support materials including templates and examples are available on the OCIO website to guide departments and other public bodies in the development of standard documents and content, supporting IM program development and management and the growth of IM capacity.

Appendices listed below directly relate to the GuideBook: IM Policy Instruments Guideline and are published independent of this document on the OCIO website, <https://www.ocio.gov.nl.ca/ocio/im/practitioners/chart.html>.

Appendix	Title
A	IM Policy Instrument Guideline – Checklist
B	Quick Reference – Records and Information Management System
C	IM Policy Instruments Listing – Template and Example
D	IM Policy Instrument Cover Page and Outline – Template and Example
E	IM Policy Instrument Inventory – Template and Example

Other GuideBook References:

- IM Governance, Accountability and Organization Guideline
- IM Education and Awareness for Employees Guideline
- IM Legal and Regulatory Framework Guideline



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – INFORMATION MANAGEMENT (IM) PERFORMANCE MEASUREMENT

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015-04-01
OCIO TRIM Number	DOC06181/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces 2009-335)
GRC Approval Date	
Related Directives	
Related Standards	
Related Guidelines	<i>See References</i>

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch	
	(name) (signature) (date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	3
2.0	Scope	3
3.0	Background	3
3.1	Measurement Principles	4
4.0	Recommended Approach	5
4.1	Identify the Activities or Components to be Measured	5
4.2	Track IM Performance Measures and Metrics	6
4.3	Complete Annual Report	6
5.0	Glossary	7
5.1	Acronyms	7
6.0	References	7
7.0	Revision History	7
	Appendix A: Sample Information Management (IM) Performance Measures and Metrics	8

INFORMATION MANAGEMENT (IM) PERFORMANCE MEASUREMENT

1.0 Overview

Performance measurement is the capture and analysis of information related to the outcome of planned goals, objectives, activities or services. Performance measurement as an ongoing process helps determine whether goals are consistently being met in an effective and efficient manner. Many components within the department's Information Management (IM) program can be analyzed on an annual basis to evaluate performance. This guideline is designed to assist public bodies in the Government of Newfoundland and Labrador to develop performance measurement strategies that support the evaluation of their IM program.

2.0 Scope

This Guideline applies to or may be used by all public bodies (hereafter referred to as departments), as defined in the *Management of Information Act*. The audience for this guideline includes all individuals responsible for the operation of an IM program within their department.

3.0 Background

Including performance measurement strategies in an IM program helps a department:

- Demonstrate the growth of IM capacity as required in the Executive performance contract;
- Evaluate both what is going well with the program, and areas that need improvement;
- Develop short and long-term plans with respect to IM program functions; and
- Maintain or adjust resource allocation based on the outcome of services or planned activities.

Departments that incorporate performance measurement in services and activities can use them as a basis for an annual report on the IM program. Potential content for an annual report may include those categories outlined below.

- Departmental Goals and Objectives for IM: Each department will have different IM goals and objectives. They will also prioritize functions differently depending on their unique legal, regulatory and operational requirements. A policy-based department may prioritize compliance initiatives where a transaction-based department may see services that support front line staff as priority.
- IM Program functions implementation/operations: Components of the IM program that are in place versus those that may need to be implemented.

- Compliance with legal and regulatory requirements: Where possible, performance measures should demonstrate that the department complies with IM legal and regulatory requirements.
- Operational support: The performance measures should demonstrate that IM functions facilitate departmental operations.
- Planned activities: The program plan will have identified activities for the year. These may include new policies, standards, guidelines, projects, tools, etc. The performance measures should demonstrate accomplishment of goals and activities.
- IM services: The provision of high-quality IM services in a timely and effective manner is an important feature of an IM program. Performance measures such as statistics on numbers of requests received and addressed, average length of time to resolve issues, and implementation of improvements to service are ways to demonstrate service quality.
- Education and awareness: Education and awareness is an easy measurement to track and helps the department to demonstrate that it is meeting its commitment to grow IM capacity.
- Variances: Performance must identify and detail variances in the IM program from the established or planned goals, objectives, activities, etc.

3.1 Measurement Principles

The success of performance measurement is dependent on the data being collected consistently and as a part of ongoing operations. Its value to the IM program is tied closely to the ability of the performance measures to provide relevant information about operations. Some basic measurement principles to consider:

- Ongoing assessment: Performance measurement must be incorporated into processes to be measured in order to consistently capture data related to a specific performance measure. Understanding the process that is the basis for the measure, training staff involved to collect data in a timely manner and then following up at milestone dates eliminates the need to scramble at the end of the year to pull together data. For example, if tracking advisory services provided by IM staff it is best to have an easy to use spreadsheet that allows them to quickly complete relevant data related to a request as it is processed, as opposed to having staff recall activities at the end of a month, quarter or year.
- Understand goals and objectives: One of the key components of the performance measurement process is the ability to demonstrate that the IM program goals and objectives are being met. Mapping each of the goals and objectives to specific measures will assist this component of the evaluation. For example if one of the annual goals for the program is to increase employee awareness of their IM responsibilities then design measures and metrics around this activity such launching a campaign to get employees to complete [IM@Work](#), the OCIO's online IM course. Having employees submit a questionnaire in return for an award will allow tracking of the % of departmental staff that have completed the course.
- Understand what is currently being tracked: There may be ways to easily get the information you need related to IM by reusing or modifying existing information gathering

processes. For example, the financial operations for the department may already have the budget allocation breakdown for the IM program.

- **Planning and management:** Performance analysis is not intended to be a full time position. However planning and time needs to be spent to understand the measures and their milestone dates to ensure that information is being gathered and reported appropriately. Follow up with the key contact staff for measured activities at milestone dates is a useful way to ensure that measurement is completed as planned.
- **Choose measures that can be transformed into valuable data:** It is not realistic to think that every IM function will be analyzed and reported on. Based on the goals, objectives, planned activities and services, choose aspects of the IM program that can be transformed into valuable data. For example, cost of third party storage is an easy to track measure because it is billed to the department on a monthly basis. This measure can be used in many ways including to justify a larger onsite storage centre if recall costs are high. When combined with other numbers, such as the volume of records destroyed (e.g. 300 boxes at the third party destroyed as per the records retention and disposal schedule) then this is used to demonstrate the fiscal value of IM.
- **Makes measurement processes reasonable:** Once the measures have been identified, ensure that the process for capturing data is easy and transparent for staff. Simply asking them to retain a monthly email folder with the final e-mail in a service thread is an easy way to incorporate the data collection into the existing process. Another example would be to have a shortcut to a tracking spreadsheet on staff desktop's so they can quickly open and insert entries. It also provides an easy means to tabulate the calls on a monthly, quarterly or annual basis.
- **Engage the right people:** Understanding the processes to be included in measurement and then making sure that the staff involved sees the value and buy into the process is critical if reliable and consistent performance data is to be collected.
- **Communications:** Communications is important to ensure that the staff relied upon to gather information and report on the IM program measures understand what they need to do to it in a consistent and timely manner as a part of ongoing operations.

4.0 Recommended Approach

4.1 Identify the Activities or Components to be Measured

There is likely extensive information available to assist in the identification of activities or components of the IM program to be included in the performance measurement process.

- **IM vision, mission and guiding principles:** The OCIO Guideline *Information Management (IM) Vision, Mission and Guiding Principles* describes the development of this information for the department. The overall purpose of performance measurement is to demonstrate that the department is supporting its IM vision, mission and guiding principles;
- **Departmental governance, accountability and organization:** The Department's IM Governance Framework, Accountability and Organizational Structures provide areas that can be analyzed. The OCIO Guideline *Information Management (IM) Governance, Accountability and Organization* outlines the development of these areas of the IM program;

- Departmental Reports: Departmental reports including audit reports, annual plans, etc. may provide measures that the IM program must support;
- Information Management Capacity Assessment Tool (IMCAT) Report: Departments that have completed an IMCAT may use the final report to provide a baseline at the beginning of their program and to identify performance measures;
- IM program plan: The IM program plan, as outlined in the OCIO Guideline *Information Management (IM) Program Plan* will identify IM services and also planned activities for the year. The ability to report against these services and activities is a major component of the performance report; and
- Departmental IM Service Catalog: An IM service catalog will include a listing of all services and contacts for each.

4.2 Track IM Performance Measures and Metrics

Prepare a summary listing of the activities to be measured that can be used to track the process. A *Sample Information Management (IM) Performance Measurement Summary* has been included in Appendix A. Update this listing as required through the year. Elements to track may include:

- Performance measure: A performance measure is the element of the IM program that is to be measured;
- Performance metric: Identify the unit of measurement used to evaluate the performance measure;
- Description: Describe the performance measure, why it is important, how it is measured and why it demonstrates value;
- Milestone: Identify important dates related to the performance measure and ensure that there is follow-up with contact staff on or around these dates. Tracking throughout the year will eliminate the effort required at year end; and
- Contact Staff: Identify the staff that are involved in the process and are able to provide information.

In order to clearly understand the measures and metrics it is important to understand the processes involved. Working with the staff responsible for the process and those who perform the work, incorporate data collection in an easy way into the existing process.

4.3 Complete Annual Report

At the end of each year, use the Performance Measurement Summary to create an annual IM Program Performance Report. The purpose of this report is to:

- Demonstrate that the program is administered properly;
- Demonstrate that the department has adhered to its IM Vision, Mission and Guiding principles;
- Outline how IM has supported compliance with departmental legal and regulatory requirements;
- Identify how IM adds value to departmental operations;

- Explain variances in what was planned and actually completed; and
- Suggest activities, services, improvements that can be included in next year’s program plan.

5.0 Glossary

5.1 Acronyms

IM	Information Management
IMCAT	Information Management Capacity Assessment Tool
OCIO	Office of the Chief Information Officer

6.0 References

[Management of Information Act](#)

Information Management and Protection Policy, TBM 2009-335

OCIO Guideline – Information Management (IM) Governance, Accountability and Guiding Principles

OCIO Guideline – Information Management (IM) Legal and Regulatory Framework

OCIO Guideline – Information Management (IM) Program Plan

OCIO Guideline – Information Management (IM) Vision, Mission and Guiding Principles

7.0 Revision History

Date Reviewed	Reviewed By
2011-03-03	Iris Power, Director of Information Management Services
2011-04-13	Shelley Smith, Executive Director Information Management
2011-04-29	Information Management Standards Board (IMSB)
2011-05-06	Government Records Committee (GRC)
2015-04-01	Bun Power, IM Consultant, IM Services

Appendix A: Sample Information Management (IM) Performance Measures and Metrics



Sample IM
Performance Measure



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – EDUCATION AND AWARENESS FOR INFORMATION MANAGEMENT (IM) PRACTITIONERS

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2009-335** approved by Treasury Board on November 19, 2009. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of Information Management programs. Guidelines generally clarify what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2016 03 31
OCIO TRIM Number	DOC03311/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2009-335
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	
Related Guidelines	Information Management (IM) Education and Awareness for Government Employees

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0 Overview3

2.0 Scope.....3

3.0 Background3

 3.1 Roles and Responsibilities4

 3.2 Education Versus Awareness5

 3.3 What is a Competency?5

 3.4 Funding for Education6

 3.5 The Information Management Competency Assessment Tool6

4.0 Recommended Approach.....7

 4.1 Education.....7

 4.2 Awareness.....8

5.0 Glossary9

6.0 Acronyms9

7.0 References.....9

8.0 Revision History9

EDUCATION AND AWARENESS FOR INFORMATION MANAGEMENT (IM) PRACTITIONERS

GUIDELINE

1.0 Overview

Support for ongoing education and awareness for Information Management (IM) practitioners is a fundamental element of the overall IM program. It ensures that employees at all levels meet the technical competencies appropriate to their role. It also ensures that practitioners are aware of existing and new policies, standards and requirements related to IM so that they can incorporate this knowledge into relevant areas of the IM program. Finally, support for IM education and awareness is an excellent way for departments to demonstrate their commitment to improved IM capacity building. This guideline assists departments to:

- Understand processes and resources that support education and awareness for IM practitioners; and
- Support development of education and awareness planning for individual IM practitioners.

2.0 Scope

This Guideline applies to or may be used by all public bodies, as defined in the [Management of Information Act](#). Reference to department in this Guideline can be understood to include any public body. The audience for this guideline includes individuals responsible for:

- The operation of a records and information management program within their department; and
- Individual IM practitioners.

3.0 Background

Education and awareness are essential for all IM employees to ensure that they have the expertise required to perform their duties effectively and stay up-to-date on new policies, standards and requirements in their area of practice. From a departmental perspective, it is critical that the IM practitioners who support the IM program are providing appropriate guidance/service to other employees. Maintaining a high-level of IM expertise within the department facilitates compliance with legal and regulatory requirements as well as overall business efficiency. Finally, support for education and awareness of IM practitioners enables the department to demonstrate it is meeting its commitment to continued IM capacity growth.

3.1 Roles and Responsibilities

There are a number of resources that are engaged in developing education and awareness for individual IM employees. First and foremost, IM practitioners, like all employees, should take responsibility for their own professional development, and take the initiative to identify the resources available to them. Additionally, they should develop their learning plans to assist them in their own career goals and success. Resources available include:

- *The Centre for Learning and Development (CLD)*: The CLD provides leadership in learning and development opportunities. The CLD coordinates the development and implementation of individual employee learning plans. A learning plan is a document that links learning opportunities to current and future job performance. The learning plan is prepared annually with the guidance of the CLD, Strategic Human Resources Management and the employee's manager. Decisions made related to funding for training are often driven by the content of a learning plan. Contact the CLD for more information regarding learning plans.
- *Strategic Initiatives (Strategic HR Division)*: Strategic HR coordinates with departmental contacts on the departmental learning requirements and allocation of the annual Organizational Development Initiatives (ODI) fund. Each year the department submits to HR a list of training priorities for the coming year. The focus of this fund is on improving technical competencies which are not typically funded through the CLD. This group also consults on employee learning plans, particularly with regard to improving technical competencies
- *Departmental Organizational Development*: Each department has an employee that coordinates the planning and use of its ODI fund. This fund is allocated on an annual basis in consultation with Strategic HR to provide for technical competencies. How involved the ODI manager is with individual employees and in their learning and development will vary by department. Activities may include:
 - Assist employees with competency assessment tools like the self-assessment or peer assessment available via the CLD,
 - Coordinate delivery of training on behalf of the department,
 - Work with departmental management team to identify and prioritize training requirements,
 - Prepare annual ODI funding request for submission to Strategic HR.
- *Departmental IM Managers*: Departmental IM managers are responsible for supporting their employees by assessing competency levels, identifying requirements and the implementation of individual learning plans; and by encouraging the employees to develop their learning plans and take responsibility for their own professional development.
- *Departmental IM Practitioners*: Individual employees are responsible for taking control over their own learning and development. This includes development and implementation of individual assessments and learning plans on an annual basis.

3.2 Education Versus Awareness

Education is the process of imparting knowledge, skill and judgment. Education generally results in new or enhanced skills that permit an employee to perform their job with greater competency and confidence. Education in a corporate setting tends to follow principles of adult education. First, learning requirements and objectives are identified. What follows is the development of a structured program to support the transfer of knowledge to a specific audience. Examples of education include:

- In-class or online training
- Seminars or webinars
- Conferences or workshops

Awareness is becoming conscious, informed or knowledgeable about components of the IM program or best practices. Awareness is often used to reinforce education (e.g. job aids or quick references are emailed to employees following a training session). Awareness may also be used simply to disseminate new tools, processes, policies, guidelines, etc. Examples of awareness include:

- Presentations
- E-mail to departmental employees
- Posters/Pamphlets
- Stickers/Mouse pads

3.3 What is a Competency?

Education and awareness are used to improve competency. A competency is a combination of experience, knowledge and understanding, skills and abilities that a person brings to a job. There are two types of competencies:

- *Core Competencies*: Core competencies are skills that are common across all departments and all functions. They form a basic foundation for all employees within the government. They are transferrable to other organizational units or job functions. Some examples are communications, service delivery, conflict resolution, self-management, ethics and professionalism. Education related to core competencies is centrally coordinated by the CLD. IM is considered to be a core competency that all government employees must develop and maintain. The Guideline *Information Management Education and Awareness for Government Employees* is used to develop this area of the IM program.
- *Technical Competencies*: Technical competencies are skills that are required to support a specialized job function. For example, there are specific competencies associated with IM roles. Education related to technical competencies is coordinated by the individuals that manage departmental ODI. This is typically an ODI contact within the department and a representative from the Strategic HR Management division.

Determining whether education supports either a core or technical competency is not always straightforward. This is because the same subject can be a core competency for one employee and a technical competency for another. For example, budgeting is a competency

that all managers must have. For a financial analyst however, more detailed knowledge of budgeting is required. For that employee, the training supports a technical competency.

IM is similar in that all employees, managers and directors require a foundation in IM principles to ensure that requirements are met. Resources are available to support IM as a core competency for these employees. Employees whose jobs are directly related to IM require educational support for IM as a technical competency.

3.4 Funding for Education

There are two options for funding education for government employees. These are:

- *CLD Funded Training*: Education related to the core competencies is coordinated and/or delivered through the CLD. There is no direct cost to departments for this training.
- *ODI Funded Training*: Each department identifies its own needs for training related to technical competencies on an annual basis. There is typically a manager assigned in each department to coordinate development and execution of the annual ODI funding.

The CLD works with individual employees to develop and pursue an annual learning plan that may identify both core and technical competencies. Funding for this annual plan is analyzed on a case by case basis to determine the appropriate source for funding.

3.5 The Information Management Competency Assessment Tool

In 2007, the OCIO identified the need for a horizontal review to assess the current structure, capability and competencies of IM across Government and to provide recommendations for advancement. The Information Management Horizontal Review (IMHR) produced important education-related assessment tools and resources designed to standardize the IM profession across government. When used properly, these tools and resources can become an important part of a departmental IM Education and Awareness program. These include:

- *Information Management (IM) Position Classification Specifications*: Use of six standard IM position classifications allows departments to set a benchmark for current and future skills of IM employees.
- *The Technical Competency Framework for Information Management (IM)*: The Technical Competency Framework is based on both industry standards and on an assessment of competency needs within the Government of Newfoundland and Labrador. Competencies are broken down into four main competencies with each further sub-divided into specific areas of expertise.
 - Information Management (IM) Practices
 - Risk Management Competencies
 - Information Protection (IP) and Security Competencies
 - Information Technology (IT) Competencies

Managers use the competencies to identify the behaviors their employees must exhibit to support organizational priorities. Employees can use the competencies to identify their own priorities for learning and development.

- *Information Management (IM) Competency Assessment Tool:* The CLD developed an assessment tool to support the use of the IM Technical competencies for learning and development by government employees. It follows the same format and methodology as similar tools deployed by the CLD. The assessment tool consists of two parts; A managers assessment checklist and an employee self-assessment checklist. Each stakeholder in the process completes his or her own checklist. Results are compared to identify how existing behaviors can be modified to support both departmental priorities and individual learning and development. These competencies are maintained by the CLD.
- *Learning and Development Resources:* The OCIO maintains a listing of learning and development resources to support the development of the IM Technical Competencies. Resources include:
 - Professional or academic courses or programs
 - Industry Certifications that support IM
 - Legislation related to IM
 - Online resources including websites
 - Books or journal articles related to IM
 - Industry associations that support the development of IM

Resources are available on the [IM Community Online](#) website.

4.0 Recommended Approach

4.1 Education

Employees should complete a learning plan each year that identifies their learning priorities and opportunities. Learning plan forms are available on the CLD website. IM practitioners can use the following steps in accessing the tools to complete the annual learning plan process:

Step 1: Review position classification descriptions to confirm that they are working at the appropriate level and identify required skills.

Step 2: Review the technical competency framework for a detailed description of the position.

Step 3: Complete the IM Competency assessment forms for both the manager and the employee.

Step 4: Identify learning resources to support the areas identified through the competency assessment process.

Step 5: Employee to complete the learning plan form, manager to review and sign-off on content.

Step 6: Employee to submit the learning plan to the CLD and book consultation to discuss services that the CLD can provide.

Step 7: Manager to provide learning requests to the departmental ODI manager for consideration in the annual budget.

Step 8: Employee to work with various stakeholders to action learning plan.

4.2 Awareness

In addition to the implementation of individual learning plans, there are numerous informal ways that IM practitioners can continue to grow their IM capacity. These include:

IM Community: The OCIO supports ongoing awareness for IM practitioners by coordinating the IM community. The IM Branch supports the IM Community by bringing together IM representatives from across the public sector. Meetings are scheduled quarterly and include presentations related to ongoing projects, best practices and standards. Employees engaged in Information Management on behalf of departments and public bodies are encouraged to attend.

IM Community Online: The IM Community Online is a secure website used by the IM community to share resources. Access is restricted to IM community members. A username and password is required to access this site and can be obtained from the IM Branch, OCIO.

Professional Associations: There are numerous associations that focus on the practice of IM that provide valuable resources to members. [ARMA international](#), for example provides members with access to documentation via their website, discounted print materials and organized events including conferences, lunch and learn, etc. via [ARMA Canada](#) or the local [Terra Nova Chapter](#).

Conferences and Symposiums: Conferences and symposiums provide employees with the opportunity to network with other IM professionals, attend information session featuring content related to case studies, new technologies or standards and best practices.

Independent Research: One of the best ways to maintain awareness is to allow time for independent study of industry materials. The IM Community Online has a list of useful resources including books, journals and websites.

Mailing lists: Participating on an ongoing mailing list to be notified of new information from industry or government sources is a useful way to ensure that employees are informed of new developments in IM.

Reference Materials: There are several venues at which IM related materials may be referenced or borrowed:

- The Legislative Library, Centre for Learning and Development and Strategic Human Resources Management all maintain lending libraries that have content useful to IM professionals that can be borrowed.
- The public library system as well as that of Memorial University, The College of the North Atlantic and Grenfell College provides reference resources that can be used for independent study.

5.0 Glossary

[Information Management](#)

6.0 Acronyms

ARMA	Association for Records Managers and Administrators
CLD	Centre for Learning and Development
IM	Information Management
IMCAT	Information Management Capacity Assessment Tool
IMHR	Information Management Horizontal Review
IP	Information Protection
IT	Information Technology
OCIO	Office of the Chief Information Officer
ODI	Organizational Development Initiatives

7.0 References

[The Management of Information Act](#)

[The Centre for Learning and Development](#)

[Strategic Human Resources Management](#)

OCIO Guideline Information Management (IM) Education and Awareness for Government Employees

8.0 Revision History

Date Reviewed	Reviewed By
2011-02-10	Iris Power, Director of Information Management Services
2011-02-14	Shelly Smith, Executive Director Information Management
2011-02-14	Information Management Standards Board (IMSB)
2011-03-17	Government Records Committee (GRC)
2016-03-31	Bun Power, IM Consultant, IM Services



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – INFORMATION MANAGEMENT (IM) EDUCATION AND AWARENESS FOR GOVERNMENT EMPLOYEES

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of Information Management programs. Guidelines generally clarify what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015-03-31
OCIO TRIM Number	DOC04593/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	
Related Guidelines	Information Management (IM) Education and Awareness for IM Practitioners

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch	
	(name) (signature) (date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	1
2.0	Scope	1
3.0	Background	1
3.1	Education	2
3.2	Awareness	2
4.0	Recommended Approach	2
4.1	Define Roles and Responsibilities	2
4.2	Identify Education and Awareness Requirements	3
4.3	Identify Tools and Venues	3
4.4	Annual Planning	4
4.5	Implementation	5
4.5.1	Analysis and Development	5
4.5.2	Education	6
4.5.3	Awareness	7
5.0	Glossary	8
6.0	Acronyms	8
7.0	References	8
8.0	Revision History	8
	Appendix A: Sample Tools and Venue Tracking Tables	9
	Appendix B: Sample Education and Awareness Plan	10
	Appendix C: Sample Orientation for New Employees	11

INFORMATION MANAGEMENT (IM) EDUCATION AND AWARENESS FOR GOVERNMENT EMPLOYEES

GUIDELINE

1.0 Overview

Education and awareness is an important component of an Information Management (IM) program. IM is a core competency that all employees within the Government of Newfoundland and Labrador must develop and maintain. Incorporating a strategic approach to education and awareness enables departments to comply with IM requirements and increases overall IM capacity. The Information Management (IM) Education and Awareness for Government Employees Guideline (hereafter referred to as the *Guideline*) assists departments to implement an IM education and awareness plan for government employees.

2.0 Scope

This *Guideline* applies to or may be used by all public bodies, as defined in the [Management of Information Act](#). Reference to department in this *Guideline* can be understood to include any public body. The audience for the *Guideline* includes individuals responsible for:

- The operation of a records and information management program within their department;
- Departmental communications staff;
- Departmental organizational development staff.

3.0 Background

Education and awareness must be recognized as an important component of the IM program. Without education and awareness:

- Employees may not understand their IM responsibilities as public employees;
- IM practices may be inconsistent across the department;
- Employees may not be aware of new policies, standards and guidelines related to IM.

Education and awareness are used to improve employee competency. A competency is a combination of experience, knowledge and understanding, skills and abilities that a person brings to a job. IM is considered to be a core competency that all government employees must develop and maintain. Additional competencies are required for departmental employees who are IM practitioners. The *Guideline – Information Management Education and Awareness for IM Practitioners* is used to develop this area of the IM program.

Guideline – Information Management (IM) Education and Awareness for Employees

3.1 Education

Education is the process of imparting knowledge, skills and judgment. Education generally results in new or enhanced skills that permit an employee to perform their job with greater competency and confidence. Education in an organizational setting tends to follow principles of adult education. First, learning requirements and objectives are identified. What follows is the development of a structured program to support the transfer of knowledge to a specific audience. Examples of education include:

- In class or online training
- Seminars or webinars
- Conferences or workshops

3.2 Awareness

Awareness is becoming conscious, informed or knowledgeable about components of the IM program or best practices. Awareness is often used to reinforce education (e.g. job aids or quick references are emailed to employees following a training session). Awareness may also be used simply to disseminate new tools, processes, policies, guidelines, etc. Examples of awareness include:

- Presentations
- E-mail to departmental employees
- Posters/Pamphlets
- Stickers/Mouse pads

4.0 Recommended Approach

4.1 Define Roles and Responsibilities

Having a clear definition of the roles and responsibilities related to IM education and awareness for employees is critical to planning and implementation. Some of the important responsibilities to be defined include:

- Who is responsible for education and awareness for the department and what will their role be?
- Who needs to approve education and awareness activities and associated deliverables? This may not be solely the responsibility of the senior manager responsible for IM.
- Who will develop, approve and oversee implementation of education and awareness activities?
- Who needs to be engaged and when?

Participants in the awareness function that may need their roles defined include:

- Senior Manager responsible for IM Employees
- Departmental Communications staff

Guideline – Information Management (IM) Education and Awareness for Employees

- Departmental Organizational Development staff
- Additional departmental resources as required

4.2 Identify Education and Awareness Requirements

Identifying the needs for education and awareness is the first step in developing a plan. Questions that must be answered include:

- What are the components of the existing IM program? Are there existing Education or Awareness materials to support these?
- Have employees been directed to the OCIO IM education and awareness resources?
- What IM activities have been identified as a priority by the department?
- Are there departmental IM tools that require education or awareness at this time? Are there any planned?
- Where are the gaps related to IM education and awareness in the department?

Sources for this information may include:

- Results of an Information Management Capacity Assessment (IMCAT)
- Consultation with IM staff, management team, etc. to understand where they see priorities

4.3 Identify Tools and Venues

Education and awareness relies on venues and tools that best support the content that needs to be delivered to employees.

Venue: A venue is the location or vehicle used for the delivery of Education or Awareness materials. Examples of venues may include:

- Department-wide meeting
- Management team meeting
- Senior management briefing

When identifying venues, helpful information for planning includes:

- Key contact responsible for planning agenda and scheduling session
- Audience (e.g. all managers and directors)
- Purpose of the venue
- Frequency (e.g. monthly, quarterly, bi-annual, annual, etc.)
- How useful has a particular venue been in the past?
- Are there departmental requirements for how these individuals are engaged?

Tools: A tool is a product that supports education and awareness initiatives. Examples of tools may include:

Guideline – Information Management (IM) Education and Awareness for Employees

- Intranet or internet content
- Job aids
- Departmental e-mails
- Posters
- Newsletters

When identifying tools, helpful information for planning includes:

- Departmental and government contacts that must be consulted (e.g., communications, program area)
- Who needs to approve content (e.g. Deputy, CEO)
- Costs associated with production
- Estimated turnaround time
- How beneficial has their use been in the past?
- Are there departmental requirements for how these individuals are engaged?

Maintaining a listing of venues and tools as a reference is recommended. Having identified both appropriate tools and venues, planning for implementation to departmental employees may begin. Sample tracking sheets for Tools and Venues have been included in Appendix A.

4.4 Annual Planning

An IM education and awareness plan will identify and coordinate activities and support the metrics gathering and reporting needed to demonstrate that IM capacity has been increased. It will also provide the direction needed to focus on specific initiatives. It is likely that one or more planning sessions with identified stakeholders will be required to complete this plan. Elements that may be included are:

- *Overview of the Current Environment:* Outline where IM education and awareness is to date. At the outset, findings from the Information Management Capacity Assessment (IMCAT) may provide a synopsis. Use reports and metrics from previous years as a basis.
- *Objectives:* What are the objectives of IM education and awareness? These objectives can be used to identify priority areas and to evaluate the effectiveness of the program.
- *Roles and Responsibilities:* Roles and responsibilities need to be defined for:
 - Executive responsible for Departmental IM Program
 - Departmental IM employees
 - Departmental Organizational Development staff
 - Departmental Communications staff
- *Standard Approach:* Identify how different types of education and awareness requirements will be handled. Consider existing departmental protocols, past

Guideline – Information Management (IM) Education and Awareness for Employees

experiences, geographic restrictions, etc. Defining a standard approach will make it easier to deal with new business as it appears and will ensure consistency in the way information is processed.

- Standard approach to developing education and awareness within the department
- Standard approach (if any) to disseminating new government-wide policies, standards, guidelines, etc.
- *Identify/Prioritize Departmental Needs:* Based on the earlier analysis, provide a list of the education and awareness needs along with where they are seen as a priority.
- *Planned Activities:* Identify the activities planned for this year based on priorities, objectives, etc. Include activities, sequence, resources and target dates, etc.
- *Reporting and Metrics:* Determine how metrics related to the success of the program will be gathered (e.g. survey's to gage IM awareness, interview with employees, etc.). How will this information be reported, when and to whom?

A *Sample Education and Awareness Plan* is included in Appendix C. This document should be updated annually or as required and provided to appropriate stakeholders.

4.5 Implementation

4.5.1 Analysis and Development

Developing and delivering new educational and awareness products specific to departmental requirements requires resources. In the annual plan, a high-level strategy for the development of new materials was identified. Some questions to ask before developing new departmental training include:

- Has this initiative been identified in the annual plan?
- What is the timeline for the implementation?
- What are the objectives of this initiative? How will these translate to learning objectives?
- Is internal development the only or best possible option? The OCIO, professional associations, industry organizations, educational institutions, etc. may be able to fill the need with existing materials, programs or offerings.
- Is this an IM initiative on which the IM resource must take a lead role (e.g. new records policy) or a program responsibility with an IM component (e.g. new process for processing applications)?
- What kind of support is needed to ensure that the departmental initiative is successful – education, awareness or a combination of both? To answer this, look at the level of change that the new initiative will require on the part of the employees, level of priority it has been given, etc.
- What tools and venues will best support the education and awareness of the initiative? Factors such as the breadth and nature of the content, magnitude of change, location of employees, etc.

Guideline – Information Management (IM) Education and Awareness for Employees

- In addition to the known stakeholders, are there departmental employees (e.g., managers, subject matter experts) that need to be engaged in the development, planning and delivery process?
- Is there an additional financial requirement that has not previously been identified?

When developing education and awareness materials:

- Ensure that all stakeholder have been identified and are engaged as appropriate
- Establish and validate the objectives in the beginning of the development process and again at appropriate intervals
- Engage appropriate resources to review or test the deliverables as required

4.5.2 Education

Education related to government IM requirements is considered to be a core competency that all employees must have to do their jobs. The CLD, Strategic Human Resources and the OCIO work together to ensure appropriate information is accessible to employees.

The goal is not to transform all government employees into IM professionals. However, because employees are individually accountable for the information they generate/receive on behalf of the government, it is important that they are provided with the information they need to meet these obligations. Strategic Human Resources includes a limited amount of IM in their government-wide orientation. It is recommended that each department review this information as a part of its own orientation and augment its content with specific departmental information as required.

Orientation is one of the most important components of the IM program. Without orientation employees are not aware of their responsibilities related to IM. A sample slide deck has been included in Appendix A. From an IM perspective it is important that all employees:

- Understand IM basic concepts and their responsibilities as government employees. Ensure that each employee completes [IM@Work: Making Information Management Work for You](#). This training is available on the OCIO website.
- For those at a management level there is additional information available through the resource management package *Information Management: A Guide for Managers and Directors*.
- Understand any departmental IM policies, procedures or tools. This will ensure that day to day IM procedures are consistent. These are set by the departmental IM group.
- Understand any specific IM requirements related to their business process. This is determined by the business unit management team.

Educating existing employees also needs to be incorporated into the annual plan. The amount of education that employees require varies. At a minimum, existing employees need to be provided with the same information listed above that is provided to new employees during orientation. One option to do this would be to provide materials to be disseminated by the management team at scheduled meetings (e.g. annual planning session, monthly team meetings). At this time employees can also be encouraged to complete the IM@Work training module. Incentives for employees to complete the program are helpful (e.g. employees that complete a feedback form are entered into a draw for a prize).

Guideline – Information Management (IM) Education and Awareness for Employees

4.5.3 Awareness

Awareness is used to:

- Reinforce what employees learn in orientation
- Communicate new requirements including policies, standards and guidelines
- Communicate new IM tools including departmental classification, records retention and disposal schedules, etc.
- Communicate events like a departmental clear-out day
- Share success stories

When the awareness program begins one of the components that can be provided is information on the existing IM related awareness available via the OCIO, professional associations, industry organizations, etc. On an annual basis awareness can be provided to employees when required to support new initiatives, projects, policies standards and guidelines. Some tips to be used in IM awareness include:

- Monitor the OCIO website for new initiatives/content that would be helpful for employees
- Leverage OCIO-produced campaigns and marketing materials including brochures, pamphlets, etc.
- Ensure that messages are timed appropriately to ensure maximum effectiveness/impact. For example, promoting a clear out day in December when business slows may have a better response than at a very busy time of year.
- Engage appropriate resources to help create or distribute information. Employees are more likely to take the time to review material if it comes from recognized leaders including senior management or subject matter experts

5.0 Glossary

6.0 Acronyms

CLD	Centre for Learning and Development
IM	Information Management
IMCAT	Information Management Capacity Assessment Tool
OCIO	Office of the Chief Information Officer

7.0 References

[Management of Information Act](#)

OCIO Guideline Education and Awareness for IM Practitioners

8.0 Revision History

Date Reviewed	Reviewed By
2011-03-08	Iris Power, Director of Information Management Services
2011-02-14	Shelley Smith, Executive Director, Information Management
2011-02-14	Information Management Standards Board (IMSB)
2011-04-04	Government Records Committee (GRC)
2015-03-31	Bun Power, IM Consultant, IM Services

Appendix A: Sample Tools and Venue Tracking Tables



Sample Tools and
Venue Tracking Table

Appendix B: Sample Education and Awareness Plan



Sample Education
and Awareness Plan 1

Appendix C: Sample Orientation for New Employees



IM Overview for new
employees 20110125



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – PHYSICAL RECORDS STORAGE DEVELOPMENT AND USE

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2009-335** approved by Treasury Board on November 19, 2009. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2016 04 16
OCIO TRIM Number	DOC06351/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2009-335
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	
Related Guidelines	See References

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

- 1.0 Overview 1
- 2.0 Scope 1
- 3.0 Background 1
 - 3.1 Physical Records 1
 - 3.2 Storage and the Record Life Cycle 1
 - 3.3 Semi-Active Storage Options 2
 - 3.4 Imaging Active Records for Improved Access 3
- 4.0 Recommended Approach 3
 - 4.1 Complete a Needs Assessment 3
 - 4.2 Define/Validate Scope and Services Required 4
 - 4.3 Document the Life Cycle 5
 - 4.4 Create Specifications 6
 - 4.5 Develop a Business Case/Requirements 8
 - 4.6 Obtain Approval for Physical Storage Development and Use 9
 - 4.7 Procure Supplies and Services 9
 - 4.8 Define Procedures 9
 - 4.9 Communications 10
- 5.0 Glossary 10
 - 5.1 Definitions 10
 - 5.2 Acronyms 10
- 6.0 References 11
- 7.0 Revision History 11
- Appendix A: Information Life Cycle Questions 12
- Appendix B: Record Storage Locations: Procedural Considerations 12

GUIDELINE FOR PHYSICAL RECORDS STORAGE DEVELOPMENT AND USE

1.0 Overview

Under the *Management of Information Act* and Government's Information Management and Protection Policy, departments are responsible for the secure and efficient management of all records, including physical records such as paper, CDs, DVDs, photographs, film, etc. This guideline includes best practices for the development and operation of any physical records storage locations including file rooms, central filling, information service centres, and off-site departmental records storage space.

2.0 Scope

This Guideline applies to or may be used by all public bodies (hereafter referred to as departments), as defined in the *Management of Information Act*. The audience for this guideline includes all individuals responsible for the operation of an IM program within their department.

3.0 Background

3.1 Physical Records

The *Management of Information Act* defines a record as:

a correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic;

Government departments are responsible for the secure and efficient management of all records and information regardless of media. A large portion of active physical records are likely stored at personal workstations. In these cases, the department relies on individual staff to follow best practices for their management. These active records either get destroyed directly by the staff or moved into the department's records management program. Requiring that staff move active records into a central location once they have completed immediate work on them increases the likelihood that they will be managed and disposed of appropriately.

Most departments have at least one (or several) physical storage location. These may include file rooms, storage vaults, registries and service centres. The management of these locations should be overseen by the department's IM division or branch. They may be administered by departmental staff (e.g. administrative assistants) but guidance, best practices and periodic review should be completed by IM practitioners.

3.2 Storage and the Record Life Cycle

Physical records management can be a resource intensive activity. Where possible, it is advantageous for a department to minimize physical records management requirements by

developing and implementing Records Retention and Disposal Schedules (RRDS) as a regular course of business. The inclusion of IM practices in ongoing business activities facilitates the transition of records from active to semi-active to disposal status.

1. Active - An active record is a record needed to perform current operations or ongoing business matters. It is consulted frequently, and it must be conveniently available for immediate reference, either manually or via a computer system. Active records may be stored onsite or online to support the flow of business.
2. Semi-Active - Semi-Active Records are those records that do not have to be readily available in primary offices but which still need to be kept for the possibility of use or reference. These records should be stored in appropriate offsite storage facilities.
3. Disposal - Disposal of records in the Government of Newfoundland and Labrador means either secure destruction or the transfer of records at the end of their lifecycle to The Rooms Provincial Archives Division (TRPAD). As required by the [Management of Information Act](#) the recommended disposal authority for government records is a Records Retention and Disposal Schedule, approved by the Government records Committee (GRC). Detailed instruction on disposal is included in the OCIO Guideline *Disposal of Records and Information*.

The Planning and Accommodations Division, Department of Transportation and Works maintains *The Government of Newfoundland and Labrador Office Space Standard*. Developed to support the efficient use of government office space. It dictates:

Currently only active records (records which are used on average, once per month) will be accommodated within the allocated space dedicated towards office accommodations. Inactive (semi-active) records will be stored offsite according to guidelines to be developed by the Office of the Chief Information Officer (OCIO).

When identifying requirements for physical storage it is important to consider that active records should be retained onsite as per the RRDS. If the department determines that the retention period identified in the RRDS is no longer appropriate (e.g. the active period should be increased or decreased) then the RRDS can be modified via a memo to the GRC.

3.3 Semi-Active Storage Options

The OCIO promotes two options for the storage of semi-active physical records:

1. *The Provincial Records Centre*: The PRC is operated by the OCIO. It provides secure storage for government records that fall within its mandate. Records accepted by the PRC include:
 - Vital Records: defined as one that is indispensable to a mission critical business operation or essential for the continuation of an organization during or following a disaster;
 - Confidential Records: Records of a sensitive or private nature, where confidentiality is required in storage conditions;
 - Archival Records: Records which, due to their enduring value or historical significance, are to be transferred to TRPAD once they are no longer required by the department or public body;
 - Records which have longer than usual semi-active retention periods may be considered to lessen the burden of storage on departments and public bodies.

Visit the OCIO website for PRC forms and transfer instructions.

2. *Third Party Storage*: Departments are encouraged to use third party offsite storage for the storage of semi-active government records which do not meet the criteria for storage at the provincial Records Centre. Abandoned buildings, hallways, janitorial closets, basements and other similar places should not be used to store semi-active records. The Government Purchasing Agency (GPA) maintains Master Standing Offer Agreements (MSOA) with third parties for the secure storage of records. Contact your departments' financial operations officer to access the most updated MSOAs.

3.4 Imaging Active Records for Improved Access

Transforming physical records to electronic format using a scanner and software such as TRIM provides immediate access to active records. The value of having records accessible electronically may justify the cost of establishing document scanning in the department. The OCIO Guideline *Record Imaging Services* provides guidance on determining the suitability of records for imaging and establishing an imaging program.

4.0 Recommended Approach

Departmental needs for physical records storage locations and use vary depending on the information flow of core business and requirements for access and use and format of records. The following approach has elements that can be adapted to accommodate the upgrade of an existing location; however it has been developed to be used primarily if a department is developing a new storage location.

4.1 Complete a Needs Assessment

A needs assessment is required to identify the active records that require onsite physical storage. The department's program plan as described in the OCIO Guideline *Information Management (IM) Program Plan* will contain detailed information about IM services. This may prove useful in determining the role that the storage facility will play in the overall IM program.

Completing an inventory as described in the OCIO Guideline *Records and Information Inventory* is a first step in determining the volume of records that must be accessible to support ongoing operations. Requirements for records to be retained onsite should be documented including:

- Title of record series;
- Records Retention and Disposal Schedule (RRDS) identifier;
- Process or program that creates the records;
- Location of records and users;
- Existing Volume;
- Anticipated annual increase;
- Format of records
- Length of active retention (active);

- Total retention (active + semi active);

4.2 Define/Validate Scope and Services Required

Analyze the records to be retained onsite to determine the overall scope of the storage requirement. Use this to outline what types of services will be required to support ongoing access and management. Things to consider when planning onsite storage and support requirements include:

- Purpose of the Storage Location: How will the storage location fit into the overall IM Governance Framework? How will the services complement or support other services? For example, will the centre be a stand alone service that is used to provide access to active records or will the facility act as a processing hub for records being transferred offsite?
- Staffing Requirements: Does staff need to be physically located within the centre? Depending on the types of services required to support the management and use of the records it may be advantageous to physically locate IM staff within the centre.
- Type of Records: What is the business value of the records? If records are critical to business processes and need to be accessible to staff immediately to complete daily functions then there may be a business case for retaining these records securely onsite at individual work stations or offices.
- Location of Users: Where are the anticipated users located? Where the users are located has an impact on the way that service is provided. For example if users are all in the same building there are different distribution options as opposed to geographically distributed users.
- Environmental conditions: Some formats of records require specific environments to ensure the longevity and preservation of the records
- Record Use: How will the records be used? For example if the records will be removed for extended periods of time then consider the need for improved tracking and reporting of files.
- Volume of Records per Year: What is the volume of records generated per year? In determining the amount of space required, understand the existing volume as well as how much the volume increases annually, being sure to factor in the implementation of the RRDS which will result in records being disposed of on a scheduled basis. Maintenance and Storage: How will the records be received by the staff responsible for the storage location? Are there costs associated with the transfer and retrieval of files? What will staff need to do to the records when they arrive? If records are already classified, organized and filed when they arrive it will eliminate work of centre staff. If this is a service that is provided by the centre staff then a processing area will be required as well as additional supplies.
- Media or Format of Records: What is the format of the records? Are the records in paper format or will there be alternative media that needs to be accommodated? Specialized storage may be required for alternative format such as oversized maps and supplies for storage of negatives or photographs may be required. Different format of records are stipulated here, but the scanning section implies that many records should be scanned. Clarification needs to be provided.

- **Retention Requirements:** How long will records be retained onsite? Understanding the retention requirement for onsite storage is necessary to understand the total volume that will be maintained at any one time. This should be documented in the RRDS. For records in several formats, the official format should be identified in the RRDS.
- **Existing Storage Space:** Can the requirements be accommodated with existing storage space? Will the development of new storage eliminate or minimize other decentralized locations? Engage Transportation and Works staff responsible for office space allocation, planning and use to determine whether existing space can be modified or if appropriate alternative space can be identified.
- **Resource Requirements:** What is the estimated cost of establishing and maintaining the storage location? Based on the physical requirements and the service requirements estimate the overall cost of establishing and operating the storage centre. Include the physical upgrade, new shelving as well as ongoing cost for salaries, processing, courier, etc.

4.3 Document the Life Cycle

The life cycle refers to the stages through which information is managed. Information management strives to manage the records in a manner that facilitates authenticity, reliability, integrity and usability throughout all stages including:

- Planning;
- Creation and organization;
- Receipt and capture of data;
- Retrieval, processing, dissemination and distribution of data;
- Storage, maintenance and protection;
- Disposal including secure destruction or transfer to TRPAD

Documenting the typical life cycle of the records that will be stored in the location may prove helpful in finalizing requirements and developing operational procedures. [Appendix A, Information Life Cycle Review](#) includes typical questions to consider when documenting the life cycle.

4.4 Create Specifications

Working with departmental stakeholders and Transportation and Works staff, and specialized consultants where necessary, use the requirements that have been identified in 4.2 to create detailed physical specifications. Considerations include:

- Physical Location and Layout
- Shelving, Equipment and Supplies

4.4.1 Physical Location and Layout

Every department will have different needs when it comes to developing their physical records storage location. Volume of records, types of services, location of users, etc. all impact the layout and design. The following are some of the physical location and layout considerations:

- Storage is best located in centre of a building. This mitigates many issues including:
 - Physical security components;
 - No windows for unauthorized entry;
 - Prevents UV damage to records;
 - Structural weight requirements due to the load of physical records on the floor.
- Avoid locations on the ground floor or in the basement of a building due to the risk of flooding;
- Access: The location must be physically accessible.
 - If services are provided to users at the location, ensure that the location is convenient and the counter space meets accessibility requirements
 - Ensure the access to, and/or emergency exits are adequate and meet fire, safety and other regulations. .
 - The storage location must be accessible by public courier as records may be shipped to it and retrievals made from it.
- Fire suppression requirements must be evaluated and implemented.
 - Ensure the fire suppression system is appropriate for the area.
 - Regulations may affect elements of the floor plan, such as the width of the aisles, the height of the stacks, sprinkler requirements, and placement and specifications of portable fire extinguishers, interior fire hoses, fire alarms, and exits.
- Lighting: Ensure the placement and levels of lighting are conducive to the work performed in the storage location.
- Electrical supply: Ensure that there are sufficient electrical outlets to power equipment. Avoid spreading cords or cables across the floor as these may become health and safety risks.
- Temperature and Humidity: Temperature and humidity levels should be appropriate for the type of media stored within the location. Inappropriate temperature and humidity may lead to the deterioration of records, particularly alternative media such as photographs and film.
- Protective coverings are recommended for open shelving to protect against damage in the event that the sprinkler system is activated, dust accumulation, etc.
- Additional security measures such as an inner secured room located within the storage location for vital or sensitive records.
- A staging area used by staff to receive and process records. The size will be dependant on the anticipated volume of records and the number of staff.

- Allocate space for government standard workstations for all regular staff. Allow for additional space to accommodate temporary workers;
- Space is required for standard office equipment including photocopiers, fax machines, shredders and secure shredding boxes. The amount of space will vary depending on the number of staff and type of services provided.
- Space may need to be allocated for viewing of records depending on the type of records maintained in the storage location and the services provided (e.g. vital records should not be removed from the location and would therefore have to be accessed onsite).
- If mail services are provided from the site then areas will be required for pick-up and processing. Include an after hours mail slot to accommodate all requirements.
- The needs assessment will have identified the record series that will be stored in active storage. Included in the assessment is the existing volume based on the inventory and anticipated annual increase.
 - The height of the ceiling as well as the floor space should be considered. The ratio of 1 cubic foot of records to 1 foot of rise to 1 square foot of floor space is approximately .333 cubic feet. Applying this factor to the known elements, such as cubic-foot measurement of records, square foot measurement of floor space and the height of the shelving stack, a department can determine the approximate space requirements. The following formulas are useful in estimating space requirements for the stack area of the records centre:

Volume of records *divided by* Stack height *multiplied by* 0.333 = floor area required

Volume of records *divided by* Floor area *multiplied by* 0.333 = stack height required

Floor area *multiplied by* Stack height *multiplied by* 0.333 = volume capacity

- Based on the estimated volume of records to be maintained, validate that the location can physically withstand the weight of the records. In the estimate, do not forget to include the weight of shelving, cabinetry and equipment.
- Consider the type of signage that will be used to identify the storage location:
 - Hours of operation
 - Emergency contact
 - Directional signs that guide users from elevators, doors, etc.

4.4.2 Shelving, Equipment and Supplies

The type of shelving and equipment required will vary depending on the type of use the location will provide. A storage location that is not staffed and is used infrequently may require that records are filed in folders and stored in boxes. Shelving and tools would be required to accommodate standard size boxes. A storage location that is staffed and actively used may retain files in folders in open shelving thereby requiring additional spacing devices to properly support file folders. Reference Government Standing Offer Agreements to validate that all shelving and equipment has already been identified and meets government and industry standards.

- Floor Space: Ensure sufficient floor space for all shelving and equipment to minimize safety hazards.
- Shelving: Shelving specifications and standards have been identified in SOAs. The vendor of record provides assessment, installation and maintenance services.
- Cabinets: Depending on how records will be retained, cabinetry may be required.
- Supplies: Ensure an adequate supply of office and filing supplies to ensure efficient processing of records. This may require an increase in the regular supply budget of the IM division or branch.
- Printer/Photocopier: the size and complexity of the printer and/or photocopier unit will depend on whether printing or copying services will be provided. The cost for the unit and required space should be factored into the storage location's operating cost.
- Fax: Purchase or lease of fax machine and required space should be included in the cost of the storage location.
- Scanner: If document scanning is included in the services provided by the storage location then this should be included analysis of implementation and operating cost. The scope of the scanning and anticipated volume will impact the amount of equipment and space required to support the service.
- Document Shredder: If document shredding will be completed onsite then this cost should be included in the estimate. It should be noted that bulk shredding should be treated as a separate activity. Due to dust and noise issues, bulk shredding should not take place in the same area as staff work and records storage unless the shredder is separated by a door and has appropriate venting to remove dust.
- Secure Shredding Boxes: The amount of space required for secure shredding boxes will depend on the volume of paper records marked for destruction.

The Department of Transportation and Works is responsible for the buildings used by the Government of Newfoundland and Labrador including their physical structure and office space as well as associated capabilities and services, such as lighting, HVAC, humidity control, and fire suppression and any identified requirements should be coordinated through Transportation and Works personnel.

4.5 Develop a Business Case/Requirements

Based on this assessment prepare a description of the physical storage required, services that will be provided and all associated costs. Components may include:

- Business Need
 - Based upon an inventory and assessment of the types and volume of records needed in active storage
- Services to be Provided

- Filing, faxing, mail pick-up processing and delivery, secure disposal, etc.
- Scope of the records to be stored
 - All active records; records of only certain program areas, all media types, etc.
- Staffing Requirements
 - Staffing of the centre or management of the centre through periodic visits for record retrieval or disposal and spot checks as required
- Total Operating Costs Per Year
 - Include supplies, shelving, maintenance costs for equipment such as photocopiers, etc.
- Return on Investment
 - Savings to be accrued by freeing up office space to be used for staff or by cutting costs for commercial storage or shredding services

4.6 Obtain Approval for Physical Storage Development and Use

Requirements will vary depending on many variables including the existing space allocated (if any), required physical upgrades, and addition of new or modification of existing support services, etc. Ensure approval of the Executive for implementation expenses and ongoing operations. Verify whether other departmental stakeholders need to be engaged including departmental financial operations and human resources.

4.7 Procure Supplies and Services

Working with departmental stakeholders and Transportation and Works, identify and procure the supplies and services required to complete any upgrades or modifications to the location. There are a number of standing offer agreements related to IM that may be useful or required during this process. For example, there are agreements for shelving that include requirements analysis (e.g., measurements and estimate of number of shelves, cabinets, etc.) and installation to be completed by the vendor. Contact your Manager of Financial Operations for access to the most up to date standing offers.

4.8 Define Procedures

Establishing consistent procedures is essential in ensuring that records are managed as per legal, regulatory and operations requirement and that services are consistent.

- Services
- Operations
- Security

Considerations for the planning and development of procedures have been included in Appendix B, *Record Storage Locations: Procedural Considerations*.

4.9 Communications

Prior to the start of operations and at appropriate intervals thereafter, communicate to departmental staff:

- Purpose of the storage location
- Services offered
- How to access services including after hours (if applicable)
- Hours of operations
- Contact Information

Use the OCIO Guideline *Education and Awareness for Government Employees* to develop a communications strategy. Things to consider:

- Create a unique centre e-mail and phone number
- Ensure that information is readily available (e.g. on the Departmental Intranet if one is available)
- Consider marketing materials (e.g. posters, handouts, etc).

5.0 Glossary

5.1 Definitions

[Active Record](#)

[Disposal](#)

[Information Management](#)

[Life Cycle](#)

[Semi-Active Record](#)

5.2 Acronyms

GPA	Government Purchasing Agency
IM	Information Management
MSOA	Master Standing Offer Agreement
RRDS	Records Retention and Disposal Schedule

6.0 References

[Management of Information Act](#)

[The Evidence Act](#)

[Information Management and Protection Policy, TBM 2009-335](#)

Government of Newfoundland and Labrador Office Space Standard

Guideline – Disposal of Records and Information

Guideline – Information Management (IM) Education and Awareness for Government Employees

Guideline – Information Management (IM) Program Plan

Guideline – Record Imaging Services

7.0 Revision History

Date Reviewed	Reviewed By
2011-04-15	Iris Power, Director of Information Management Services
2011-05-13	Shelley Smith, Executive Director Information Management
2011-05-13	Information Management Standards Board (IMSB)
2011-05-25	Government Records Committee (GRC)
2016-04-16	Bun Power, IM Consultant, IM Services

Appendix A: Information Life Cycle Questions



Information Life
Cycle Questions v1.21

Appendix B: Record Storage Locations: Procedural Considerations



Records Storage
Locations Procedural

TABLE OF CONTENTS

- 1.0 Overview 1
- 2.0 Scope..... 1
- 3.0 Background 1
 - 3.1 IP Principles..... 1
 - 3.2 IP-Related Legislation 2
- 4.0 IP Stakeholders 3
 - 4.1 Permanent Heads of Public Bodies..... 3
 - 4.2 Government Employees 3
 - 4.3 Departmental IM Staff 3
 - 4.4 Departmental ATIPP Coordinator..... 3
 - 4.5 Departmental Operations 4
 - 4.6 Office of the Chief Information Officer (OCIO) 4
 - 4.7 Access to Information and Protection of Privacy (ATIPP) Office 4
 - 4.8 Department of Transportation and Works 4
- 5.0 Recommended Approaches for Building IP into an IM Program 4
 - 5.1 Understand Current IP Capacity 4
 - 5.1.1 Review legislative and policy environment 5
 - 5.1.2 Review existing documentation 5
 - 5.1.3 Identify IP roles and responsibilities..... 5
 - 5.1.4 Create a records inventory..... 5
 - 5.1.5 Identify physical, technical and administrative safeguards 5
 - 5.2 Determine IP Priorities and Objectives..... 6
 - 5.3 Document IP Processes, Protocols and Best Practices..... 6
 - 5.4 Promote Education and Awareness 6
- 6.0 Glossary 7
- 7.0 Acronyms 7
- 8.0 References..... 7
- 9.0 Revision History 8

INFORMATION PROTECTION (IP)

GUIDELINE

1.0 Overview

Information Protection (IP) is an area of practice focused on the protection of information from inappropriate access or use, using a variety of means as required; including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. Information Protection represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, public bodies are required to protect information as part of their accountability under Section 6 of the [Management of Information Act SNL2005 c.M-1.01](#).

2.0 Scope

This Guideline applies to or may be used by all public bodies, as defined in the [Management of Information Act](#). Reference to department in this Guideline can be understood to include any public body. The audience for this guideline includes individuals responsible for the operation of an IM program within their department. There are several guidelines that relate to the development and implementation of Core IM Foundation and IM Program Components. This Guideline supplements the OCIO Guideline *Information Management (IM) Program Plan* by providing IP guidance and best practices that should be incorporated into a department's overall IM Program

3.0 Background

The [Management of Information Act](#) requires that all public bodies develop, implement and maintain a records (information) management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records. IP is an important component of any IM program and typically includes:

- An understanding of Government's legislative and policy environment;
- An understanding of Government-wide IP Directives, Standards and Guidelines released by the Office of the Chief Information Officer (OCIO);
- An inventory of information assets containing sensitive and/or critical information
- Physical, technical and administrative security safeguards; and
- IP education and awareness.

3.1 IP Principles

IP promotes the protection of Government information by understanding information sensitivity and criticality and placing reasonable safeguards around information relative to its sensitivity criticality; the more sensitive the information, the more safeguards should be put in place to protect that information. Information sensitivity and criticality can be determined

by evaluating the information's value to an organization based on its Confidentiality, Integrity and Availability requirements.

- **Confidentiality** - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes; upholding required restrictions against unauthorized access or disclosure of information.
 - Includes personal information, as defined under s.2 the *Access to Information and Protection of Privacy Act (ATIPPA)*.
 - Includes personal health information, as defined under s.5 the *Personal Health Information Act (PHIA)*
 - As a general rule, any information which would be exempt from public access under s.18 – 30 of the *ATIPPA* should be considered confidential.
- **Integrity** - The property of safeguarding the accuracy and completeness of information; maintaining the authenticity and preventing unauthorized modification or destruction of information.
 - Includes information used to make business decisions
 - Includes information used for legal or court purposes.
- **Availability** - The property of being accessible and useable upon demand by an authorized entity; Ability to perform its required function at a stated instant/period of time; ensuring timely and reliable access to and use of information.
 - Includes information required for Business Continuity.

All information that is collected and maintained by the government must be securely managed. It is important to understand the types of information maintained by a department. When implementing IP best practices into an overall IM Program, a department should identify sensitive and critical records in their possession.

3.2 IP-Related Legislation

Implementation and promotion of IP best practices within an overall IM Program are dependent upon a clear understanding of several key pieces of Government of Newfoundland and Labrador legislation, such as the:

- *Management of Information Act* - requires each department to protect information as a part of its ongoing IM program.
- *Access to Information and Protection of Privacy Act (ATIPPA)* - requires each department to provide an open right of access to government information, with specific and limited exceptions, and promote access to and protection of personal information in the custody or control of the department. For more information about the responsibilities imposed on a department under the ATIPPA, visit <http://www.justice.gov.nl.ca/just/info/index.html> or contact the ATIPP Office, Dept of Justice.
- *Personal Health Information Act (PHIA)* – this health-sector specific privacy legislation governs the manner in which personal health information may be collected, used and disclosed within the health care system and creates a consistent approach to protecting personal health information across the health care system, in both the public and the private sectors. For more information about the responsibilities imposed on a

department under PHIA, visit <http://www.health.gov.nl.ca/health/PHIA/> or contact the Department of Health and Community Services.

- *Evidence Act* - requires that records are authentic, reliable and usable to act as evidence of government's business activities.
- *Departmental and Other Legislation* - Government business is often driven directly by legislation. In addition to the above mentioned Acts, departments may have additional requirements around maintaining the confidentiality, integrity and availability of information within departmental-specific or federal legislation. An understanding of all legislative requirements within a department is important in promoting IP best practices within an overall IM Program.

4.0 IP Stakeholders

4.1 Permanent Heads of Public Bodies

The permanent head of a public body is responsible for developing, implementing and maintaining a records (information) management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of public records.

4.2 Government Employees

A government employee includes, staff, contractors, consultants, students, temporary workers, vendors, agents, third parties and other persons entrusted to handle and/or maintain information on behalf of the department. From an IP perspective, government employees are responsible for:

- Adherence to government legislation and policies, including departmental policies and government-wide IP Directive, Standards and Guidelines issued by the OCIO
- Adherence to departmental protocols and processes put in place to protect information;
- Understanding and regularly reviewing IP guidance and best practices provided by the department and the OCIO; and
- Completion of IP training activities recommended by their department;

4.3 Departmental IM Staff

Departmental IM staff support the overall IM program. IP is an important component of an IM program. Departmental IM staff develop and implement tools that support IP and are responsible for communicating new IM and IP initiative, policies, standards and guidelines within their department.

4.4 Departmental ATIPP Coordinator

Each department has an ATIPP Coordinator that is responsible for the administration of the ATIPP Act. This an important resource from an IP perspective as they are able to advise employees on issues related to compliance with privacy and access to information requirements.

4.5 Departmental Operations

Departments may have internal staff responsible for building security and maintenance. This staff member should be engaged as appropriate in the development and implementation and enforcement of protective measures related to the physical and administrative security of information (e.g., locks on doors, cabinets, building security system or cameras, flooding, sign-in of visitors, use of security badges, etc...) This staff member will work with the Department of Transportation and works, vendors, etc. to maintain building security and maintenance.

4.6 Office of the Chief Information Officer (OCIO)

The Information Management (IM) Branch of the OCIO provides advisory services and support to the OCIO, government departments and supported public bodies on Information Management and Protection, as mandated by the *Management of Information Act*. The IM Branch is responsible for the issuance of government-wide IP Directives, Standards and Guidelines. Departments can seek advice from the OCIO in developing and implementing their IM and IP program by contacting IM@gov.nl.ca.

4.7 Access to Information and Protection of Privacy (ATIPP) Office

The Access to Information and Protection of Privacy (ATIPP) Office oversees the implementation and coordination of the *ATIPPA*. Departments should seek the advice of the ATIPP office in matters related to the protection of personal information and public right of access to government information, as defined in the *ATIPPA*.

4.8 Department of Transportation and Works

The Department of Transportation and Works is responsible for the physical security and maintenance of all government buildings. Departments, and in particular the individual responsible for the department's IM program, should establish a working relationship with Transportation and Works to ensure they work together effectively on matters related to physical security and management of spaces in which information is stored or managed.

5.0 Recommended Approaches for Building IP into an IM Program

One of the primary objectives of IP is to minimize the risk of inappropriate access to or collection, use, disclosure or disposal of sensitive government information. The following guidance will help all departments assess their current capacity to implement IP best practices and plan for improving IP capabilities within their overall IM Program into the future.

5.1 Understand Current IP Capacity

In order to have a complete view of where a department stands from an IP perspective, it may be useful to complete an environment scan of what the department is currently doing in its daily business practices. If the department has completed an Information Capacity Assessment using the OCIO's IM capacity Assessment Tool (IMCAT), much of the information required in assessing the state of IP and planning for longer term practices may already be captured and recommendations may already exist.

5.1.1 Review legislative and policy environment

Obligations around protecting information are often driven by legislation and policies. Prior to incorporating IP best practices into an overall IM Program, a department should review and assess all legislation and policies that impact the department – this may include provincial and federal legislation and well as Government-wide and department-specific policies.

5.1.2 Review existing documentation

There are several key documents within Government that can provide guidance when incorporating IP best practices into a department's overall IM Program, such as:

- Results of an Information Management Capacity Assessment (IMCAT);
- Annual, Business and Strategic Plans;
- Organization Chart;
- File Classification Plan;
- Records Retention and Disposal Schedules;
- Business Continuity Plans; and
- Privacy Breach Protocols from the ATIPP Office.

5.1.3 Identify IP roles and responsibilities

Having a clear definition of the roles and responsibilities related to IP is critical to planning and implementing IP best practices into a department's IM Program. In addition to the stakeholders identified in this document, roles and responsibilities may also exist for Senior Managers responsible for IM and ATIPP. In particular, it is important to identify who is responsible for approving IP activities and associated deliverables within a department.

5.1.4 Create a records inventory

A records and information inventory is an important tool to support the planning and implementation of IP activities within an IM Program. An inventory will enable employees to identify the volume and location of sensitive information. It will also link information to originating business units and processes; this will enable IM staff to identify employees that need to be engaged in the planning and implementation process. The OCIO Guideline *Records and Information Inventory* outlines how to complete a records and information inventory.

5.1.5 Identify physical, technical and administrative safeguards

Safeguards should be put in place relative to the sensitivity and criticality of the information they are meant to protect. Within departments, safeguards can be physical, technical or administrative in nature.

Physical safeguards monitor and control the physical work environment (e.g., locks on buildings, doors and cabinets; card access systems; video surveillance; security guards, etc...). The OCIO Guideline *Physical Records Storage Development and Use* details how to assess physical locations for proper IM.

Technical safeguards monitor and control access to electronic information and computer systems (e.g., user names and passwords, application account management, system logging and auditing, encryption, etc...). It is important to note that most technical

safeguards are maintained by the OCIO, not a department, and as such are outside the scope of this Guideline.

Administrative safeguards provide a framework for operating and managing the work environment (e.g., policies, directives, standards, guidelines and procedures; privacy and other IP-related training; security clearances and background checks; assignment of roles and responsibilities, etc.).

5.2 Determine IP Priorities and Objectives

The documentation review and the records inventory will help identify priority areas for IP within a department's IM Program. Schedule interviews as required with employees that can provide information on existing processes and requirements. This information will help to prioritize departmental IP requirements (e.g. a new Guideline is needed, a process must be reengineered, extra physical security is required around physical records, etc.).

Departmental executive should identify and approve priorities for incorporating IP best practices within a department. Based on the estimates provided by stakeholders, these priorities can be organized into a plan. This plan may require multi-year approach and incorporation of IP priorities into business, annual and strategic departmental plans is encouraged to ensure the IP focus is kept in view as the department moves forward with its business activities.

5.3 Document IP Processes, Protocols and Best Practices

Once the current state has been determined and existing documentation reviewed, it is recommended that department-specific protocols, processes, policies, standards, guidelines and best practices are developed, documented and implemented within the department. For example, a department may choose to develop specific protocols related to a privacy breach, based on the underlying principles and requirements of the ATIPP Office's Privacy Breach Protocols. The OCIO guideline *IM Policy Instruments* provides instruction on how to create new IM-related policies and standards.

5.4 Promote Education and Awareness

Disseminating existing information available through various stakeholders is a good way to kick-start an IP program. Use the *IM Education* and *IM Awareness Guidelines* to develop departmental plans around IP education and awareness.

- Encourage employees to regularly visit the OCIO website to ensure current awareness of IP guidance and best practices are understood. The OCIO website has extensive information that all employees should have right away that will educate them on IP-issues, including information about [IM@Work](#) IP Fundamentals and IP Guidelines and Best Practices.
- The ATIPP Office maintains an educational program for employees. Online training can be accessed immediately by employees through the [Access and Privacy Course for Government of Newfoundland and Labrador Employees](#). Contact the departmental ATIPP Coordinator for information.
- Communicate existing Transportation and Works policies, standards or guidelines related to facilities operation and management. Contact the departmental manager responsible for general operations for further information.

- Most importantly, the department’s approach to IP should include regular communication of IP guidance and best practices throughout the department.

6.0 Glossary

[Information Protection](#)

[Availability](#)

[Authenticity](#)

[Confidentiality](#)

[Government employee](#)

[Confidential Information](#)

[Integrity](#)

[Personal Information](#)

7.0 Acronyms

ATIPPA	Access to Information and Protection of Privacy Act
IMCAT	Information Management Capacity Tool
IP	Information Protection
OCIO	Office of the Chief Information Officer
PHIA	Personal Health Information Act

8.0 References

[Management of Information Act](#)

[Access to Information and Protection of Privacy Act](#)

[Personal Health Information Act](#)

Guideline – Information Management (IM) Program Plan

Guideline – Information Management (IM) Policy Instruments

Guideline – Information Management (IM) Education and Awareness for IM Practitioners

Guideline – Information Management (IM) Education and Awareness for Government Employees

Guideline – Physical Records Storage Development and Use

Guideline – Information Management (IM) Performance Measurement

Guideline – Records and Information Inventory

9.0 Revision History

Date Reviewed	Reviewed By
2011-02-02	Iris Power, Director of Information Management Services
2011-02-02	Shelley Smith, Executive Director, Information Management
2011-04-05	Tracey Goulding, Manager (IM Consultant), Information Protection
2011-04-07	Information Management Standards Board (IMSB)
2011-04-14	Government Records Committee (GRC)
2015-04-01	Bun Power, IM Consultant, IM Services



3. IM Tools

3.1. Records and Information Inventory	36
3.2. Classification Plan Development for Operational records	37
3.3. Records Classification Plan Implementation	38
3.4. Disposal of Records.....	39
3.5. Record Imaging Services	40



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – RECORDS AND INFORMATION INVENTORY

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)** approved by Treasury Board as well as the **ATIPP Policy**. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015 03 18
OCIO TRIM Number	DOC03306/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335) ATIPP Policy
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	Corporate Records and Information Management Standard (C-RIMS)
Related Guidelines	Classification Plan Implementation Development for Operational Records

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

- 1.0 Overview 1
- 2.0 Scope 1
- 3.0 Recommended Approach 1
 - 3.1 Planning the Inventory2
 - 3.1.1 Approval2
 - 3.1.2 Preliminary Research2
 - 3.1.3 Plan Development3
 - 3.1.4 Scope.....3
 - 3.1.5 Communication Plan3
 - 3.1.6 Staff Training3
 - 3.1.7 Work Schedule3
 - 3.1.8 Monitoring and Updating the Plan3
 - 3.2 Conducting the Inventory.....4
 - 3.2.1 Inventory Approach4
 - 3.2.2 Inventory Data Collection4
 - 3.3 Completing the Inventory.....5
 - 3.4 Understanding the Findings.....5
 - 3.4.1 Analyzing Data5
 - 3.4.2 Typical Findings and Recommendations6
- 4.0 Glossary 7
 - 4.1 Definitions7
 - 4.2 Acronyms.....7
- 5.0 References..... 7
- 6.0 Revision History 7
- Appendix A: Records Inventory Worksheet Procedure 8
- Appendix B: Records Inventory Worksheet.....12

RECORDS AND INFORMATION INVENTORY

GUIDELINE

1.0 Overview

The *Records and Information Inventory Guideline* (hereafter referred to as the *Guideline*) is used by a public body to organize and carry out an inventory of its records and information holdings. The information collected through an inventory provides the foundation for the management and protection of information assets in all formats. The inventory is a requirement in the process described in the *Guideline - Classification Plan Development for Operational Records*. Results gained through an inventory will also support decision making for records format conversion projects; leverage a public body's ability to respond to Access to Information and Protection of Privacy (ATIPP) requests; protect sensitive information; evaluate risk; increase business value of information holdings; support statutory compliance; practice due diligence for a safe work environment; and improve the use of equipment and space.

The *Guideline*:

- provides best practice for public bodies to use in gathering information about their records and information holdings; and
- assists the public body in ensuring that the information collected during the inventory process is useful and meaningful.

2.0 Scope

This Guideline applies to or may be used by all public bodies (hereafter referred to as departments), as defined in the [Management of Information Act](#). The audience for this guideline includes all individuals responsible for the operation of an IM program within their department.

3.0 Recommended Approach

The purpose of a records and information inventory is to provide adequate and meaningful information about records and information holdings that will support decision making in the management and protection of information assets.

Benefits of an inventory:

- provides primary control over records and information holdings.
- identifies and establishes proper ownership of records and information.
- assists in determining retention period for records, format(s), secure protection, destruction date, archives date, transfer date and means of destruction.
- forms a foundation for understanding records and information assets.

The information collected from the inventory identifies:

- what the records and information are;
- where they are located;
- what format they take;
- the extent (boxes, files, gigabytes, etc.);
- how they are stored and their storage conditions;
- who creates them; and
- why and how they are created, used and managed.

The inventory is one of the first IM initiatives a public body should engage in as it is a fundamental process from which many other IM decisions will be made. An inventory is a valuable reference tool when completing activities such as transferring records and information to alternate storage and media conversion; enforcing litigation holds; responding to ATIPP requests and legal discovery; conducting risk assessments; classifying information for security; preparing for TRIM implementation and other application implementation; developing plans and reporting on information management and protection; planning for equipment and space; and other information management and protection initiatives.

The inventory should document the entire records and information holdings of the public body. It should include all information assets physically and electronically stored in offices, and off-site locations as well as on computer drives, or storage devices, servers and off-site data storage repositories. This involves all levels of staff accountable and responsible for the management and protection of the information assets. The inventory process includes: devising a plan to oversee the activities; training and adapting survey tools for data collection; collecting and compiling data; and analyzing and reporting on the results

3.1 Planning the Inventory

This section defines the steps necessary for getting organized and overseeing the activities and processes involved in conducting an inventory.

3.1.1 Approval

Before beginning an inventory, a plan needs to be developed and approval sought from Executive. Success is dependent upon Executive and senior management support and knowledge transfer from staff who create and use the records. Communicating the business case and plan for an inventory is essential to garnering cooperation of staff during the project.

3.1.2 Preliminary Research

Gather information to estimate the effort and resources needed to complete the inventory.

Inventory Benchmark: One person can inventory 20-30 cubic feet of records in a day.

Obtain a current organizational chart that describes the functions of each office. Contact staff to locate records. Identify contacts that might have lists already prepared.

Compile a listing of areas that need to be inventoried and map file locations. A quick walk-through office and storage areas surveying the bulk of records is a good starting place to get an idea of the volume and the accessibility of the physical records. Flag any hazards and note any problems with records or space. This needs to be completed for all locations in which information assets are stored.

Compile a list of supplies including a flashlight, gloves and dust mask for storage areas. If necessary, estimate the cost of additional resources to be included in the plan, such as hard hats, protective footwear and clothing and more sophisticated breathing apparatus if deemed necessary.

3.1.3 Plan Development

Using the information gathered in your preliminary research, develop a plan that outlines the effort and resources necessary to complete the inventory. The plan should contain the purpose and objectives of a records inventory; a strategy outlining the scope of the inventory and how it is being done; a communications plan; a list of project staff; and the work schedule.

3.1.4 Scope

Identify the scope of the inventory and include which business units and locations will be inventoried. Typically, records are surveyed by record series related to specific business units regardless of media or format. Data is collected on worksheets and entered and tabulated in a spreadsheet.

Describe the roles and responsibilities of staff and group leaders participating in the inventory. Staff in the business unit and records staff should work together during the survey for knowledge transfer and to ensure accuracy. Consult with branches and divisions to determine what will work best for their specific business units. Program staffs are the specialists on how the records they create are used, and play a key role in understanding the needs of their division or work unit.

3.1.5 Communication Plan

When the plan is complete and has Executive approval, communicate it to Executive, senior management and staff who will be involved in the inventory. This includes a presentation communicating which areas will be inventoried, the role of staff in each area and the projected work schedules to the Executive and senior management groups; orientation and training for staff involved in the project; and a wrap-up or follow-up presentation to either or both reporting on the success of the project and its findings. The Executive should then communicate their support to staff to garner their cooperation.

3.1.6 Staff Training

Conduct training workshops with staff involved in the project. Procedures for completing worksheets and sample worksheets are in *Appendices A and B*.

3.1.7 Work Schedule

Schedule the order of divisions or work groups to be inventoried and consult with managers and supervisors to ensure that times selected are appropriate. Establish time-lines and completion dates. Adjust the work schedule as the project proceeds.

3.1.8 Monitoring and Updating the Plan

Monitor plan time-lines and update the plan as the inventory proceeds. Timelines are likely to be affected due to the abilities and availability of staff; surprises such as finding a cache of hidden records; work-safety issues; and the loss of resources such as inventory staff leaving

during process. Adjust the plan and report to Executive and senior management on a regular basis about progress and any adjustments or setbacks.

3.2 Conducting the Inventory

This section of the *Guideline* provides information on conducting the inventory process.

The scope of the inventory should include all the records and information holdings. This means all records on-site at the main office, off-site in other offices and in records storage areas, as well as all electronic records stored in shared drives, personal drives and on hard drives or external storage devices. The inventory includes active records that are used in current business processes; semi-active records that are used infrequently; and, inactive records that have served their primary business purpose and are no longer being used. Non-records, such as blank forms and reference materials, should not be included in the inventory. If they are discovered during the course of the inventory and are no longer required by the organization they may be disposed of appropriately.

3.2.1 Inventory Approach

The inventory starts out as being location and business function specific. The physical arrangement of the records provides clues as to the business function or part of a public body which owns the records.

Begin at a specific location in a room and proceed systematically following a logical progression. Mapping the room and numbering file cabinets ahead of time will be useful. Tag or label each file drawer or volume as it is inventoried. Flag vital records and those identified by the business section as having enduring value.

During the process it might be useful to note the locations of non-records and records that do not belong to the public body as an aside to be followed up on during a clean-out day. However, this information should not form part of the public body's inventory.

3.2.2 Inventory Data Collection

Information about a public body's records initially collected on an inventory worksheet ([Appendix B](#)) should then be entered into a spreadsheet. Procedures for completing worksheets are in ([Appendix A](#)). Records are generally arranged systematically by record series to follow business needs and usage. It is important to include staff working in each section to assist in the inventory because their knowledge about the records will add value to the inventory process.

The inventory is a collection of record series which are groups of identical or related records that are identifiable as a unit. Details at the folder or document level are not included in the inventory unless their identification is questionable or they have been disconnected from the business function in some way; for instance: lost in a move or found unlabelled on a shelf.

The title of the record series is typically known by the business unit that creates or uses the records. It should accurately represent the content of the record series and be distinguished from other series. From time to time, the contents of folders and other containers may be examined in order to identify the correct record series, business function, or part of the public body to which it belongs.

File and box lists can be useful for gathering information to complete worksheets; however, it is important to check the lists and the physical location to confirm that the information is accurate.

3.3 Completing the Inventory

This section of the *Guideline* provides additional information on completing and maintaining the inventory.

As each section in each physical location is completed, the worksheets should be examined for completeness. Be prepared to follow-up with staff involved in the process before entering data into the spreadsheet. Do not destroy the worksheets until information has been transferred to the spreadsheet and the accuracy of the resulting report has been confirmed by each section.

Worksheets are entered into the spreadsheet for manipulation and generating reports. It is important to generate an inventory report for each business unit as their section is completed and request feedback to ensure that the information is correct and to confirm the proper identification of their record series.

Once an inventory has been compiled, it is analyzed for making decisions about the clean-up of records and the scheduling of record series to off-site storage, disposal authorization or transfer to the archives. After performing these operations the inventory should be updated. Since the design of the inventory is by record series and most records and information management activities occur by record series, there will be less effort in updating and maintaining it.

Initially, the inventory provides primary intellectual control over the physical arrangement and location of records. Its secondary use could be expanded to support other activities with a public body's records and information holdings such as legal discovery and disposal of records. The spreadsheet could be expanded to include fields to be used for information about legal holds, ATIPP requests, and retention/disposition values from an approved records and retention schedule. The inventory results can also be imported into a public body's electronic document or records management system where one exists. At this stage the public body is ready to do its classification plan.

3.4 Understanding the Findings

This section of the *Guideline* provides guidance on effectively evaluating information gathered from the inventory including concrete examples and recommendations.

3.4.1 Analyzing Data

Information contained in the inventory can be used and tabulated for various purposes. Typically an inventory pulls together a complete picture of the public body's records and information holdings beginning with the scope, purpose and quantity of record series.

This information can be analyzed to:

- Determine which records the public body owns and identify records a department has in their possession that they do not own.
- Plan for future space and security needs.
- Conduct a risk analysis of retaining current record inventory levels or series.
- Identify gaps in records.
- Develop and implement a records classification plan.
- Support filing system improvement.

- Support creation of standard shared directory structures for electronic records.
- Develop and implement a records retention and disposal schedule.
- Plan migration and reformatting strategies.
- Assess and improve storage conditions.
- Conduct Occupational Health and Safety due diligence.
- Assess and improve information protection.
- Support business continuity planning.
- Support ATIPP and other discovery requests, collection, preservation and access.
- Enforce legal holds; and
- Support other activities relating to the management and protection of information assets.

3.4.2 Typical Findings and Recommendations

Finding/Issue	Recommendation
Old record series found in closet	If there is no Records Schedule use one time disposal.
Duplicate records	Check Records Schedule and Securely dispose of copies.
Files not adequately labeled	Develop appropriate naming conventions.
Un-labeled computer diskettes	Review diskettes content and label, include date ranges of information.
Record series found from business or program area that no longer exists	Review public body and government policy on the disposition or transfer of abandoned records.
Abandoned records from another department, agency or business unit that no longer exists	Review public body and government policy on the disposition or transfer of abandoned records.

4.0 Glossary

4.1 Definitions

[Disposal](#)

[Inventory](#)

[Record](#)

[Record Series](#)

[TRIM](#)

4.2 Acronyms

ATIPP	Access to Information and Protection of Privacy
PIPEDA	Personal Information Protection and Electronic Document Act
RRDS	Records Retention and Disposal Schedule
TRPAD	The Rooms Provincial Archives Division

5.0 References

[Management of Information Act](#)

[Access to Information and Protection of Privacy Act](#)

[Information Management and Protection Policy, TBM 2009-335](#)

[Newfoundland and Labrador Regulation 11-07](#)

6.0 Revision History

Date Reviewed	Reviewed By
2010-11-05	Access to Information and Protection of Privacy (ATIPP) Office
2010-11-22	Information Management Standards Board (IMSB)
2010-12-06	Iris Power, Director of Information Management Services
2011-01-06	Shelley Smith, Executive Director Information Management
2011-01-26	Government Records Committee (GRC)
2015-03-18	Bun Power, IM Consultant, IM Services

Appendix A: Records Inventory Worksheet Procedure

The Records Inventory Worksheet is a tool used for collecting information about a department's records and information holdings. The following sections provide further clarification on the various components indicated in the diagram below that will assist you in completing the Records Inventory Worksheet.

1. Inventoried By	RECORDS INVENTORY		2. Date
	Inventoried By (Last Name, First Name):	Date Inventoried (yyyy-mm-dd):	
3. Contact Information	Contact Information (Position, Division/Section, Telephone #, Email Address):		4. Person Responsible for Maintaining Records
	Person responsible for maintaining records (Name, Title and Telephone number):		
5. Working Record Series Title	RECORD SERIES IDENTIFICATION		6. Location of Record Series
	Working Record Series Title:	Location of Record Series:	
8. Inclusive Dates	Description: (Summary of contents; continue on reverse if required, include filing patterns)		7. Description
10. Records Status	Inclusive Dates:	Life-cycle Phase:	9. Life-cycle Phase
	From (yyyy-mm-dd): To (yyyy-mm-dd):	<input type="checkbox"/> Active <input type="checkbox"/> Semi-Active <input type="checkbox"/> Inactive	
12. Filing Method	Records Status:		11. Records Medium
	<input type="checkbox"/> Original <input type="checkbox"/> Copy		
14. Frequency of use	Records Medium (Tick all that apply):		13. Storage
	<input type="checkbox"/> Paper <input type="checkbox"/> Electronic <input type="checkbox"/> Microfilm/fiche <input type="checkbox"/> Other		
16. ATIPP Exceptions	Filing Method:		15. Volume
	<input type="checkbox"/> Alpha <input type="checkbox"/> Numeric <input type="checkbox"/> Alpha-numeric <input type="checkbox"/> Subject <input type="checkbox"/> Chronological <input type="checkbox"/> Other		
	Storage:		
	<input type="checkbox"/> Filing Cabinet (Lateral) <input type="checkbox"/> Filing Cabinet (Vertical) <input type="checkbox"/> Boxes <input type="checkbox"/> Other		
	Frequency of use:		
	<input type="checkbox"/> High (Daily) <input type="checkbox"/> Medium (Once a Week) <input type="checkbox"/> Low (Less than once a month)		
	Volume (per linear foot):		
	ATIPP EXCEPTIONS		
	Identification of ATIPP and other Exceptions to Access as Applicable:		
	<input type="checkbox"/> Not Applicable <input type="checkbox"/> Section 18 - Cabinet Confidences <input type="checkbox"/> Section 19 - Local public body confidences <input type="checkbox"/> Section 20 - Policy advice or recommendations <input type="checkbox"/> Section 21 - Legal advice <input type="checkbox"/> Section 22 - Disclosure harmful to law enforcement <input type="checkbox"/> Section 23 - Disclosure harmful to intergovernmental relations or negotiations <input type="checkbox"/> Section 24 - Disclosure harmful to the financial or economic interests of a public body <input type="checkbox"/> Section 25 - Disclosure harmful to conservation <input type="checkbox"/> Section 26 - Disclosure harmful to individual or public safety <input type="checkbox"/> Section 27 - Disclosure harmful to business interests of a third party <input type="checkbox"/> Section 30 - Disclosure of personal information <input type="checkbox"/> Section 30.1 - Disclosure of House of Assembly service and statutory office records		
	Other: Identify Federal or Provincial Acts, Regulations or Departmental Public Access Restrictions:		

1. Inventoried By

Record the name of the person doing the inventory.

2. Date Inventoried

Record the date the inventory was conducted. When inputting the date use the government date standard *yyyy-mm-dd*.

3. Contact Information

Record the position, division/section, telephone number and email address of the person conducting the inventory.

4. Person Responsible for Maintaining Records

Record the name, title and telephone number of the person responsible for maintaining the records series.

5. Working Record Series Title

Record the record series title by which it is commonly known. Should a title not exist, identify the record series by using the name of the business function, activity or class of records that it relates to or use the name of the owner of the records in the title until further research and analysis is done to confirm the record series.

6. Location of Records Series

Record the physical location of the record series. Provide additional information on multiple locations. (It might be easier to complete a separate worksheet for each location and compile information in the master inventory later.)

7. Description

Examine the records and provide a description that includes physical condition, potential conservation issues (e.g., mould) and a summary of the content including types of forms and records, repetitive forms and specialized filing patterns.

8. Inclusive Dates

Record the range of dates contained within the record series. When inputting the date use the government date standard *yyyy-mm-dd*.

9. Life-Cycle Phase

Identify the record series' life-cycle phases contained in the series on-hand that is being inventoried. Some record series might be broken out into separate locations because of the nature of its current activity. Active records might be in the immediate office area while semi-active and inactive records might be located elsewhere in the organization or stored offsite at another office or a record centre. Information provided in this section supports the development and implementation of a records retentions and disposition schedule.

10. Record Status

Record whether the series is considered to be the original or a convenience copy with the original being located elsewhere.

11. Records Medium

Identify the appropriate medium of record series being inventoried.

12. Filing Method

Identify physical filing arrangement. Provide additional information on other types of arrangement.

13. Storage

Identify types of storage in which the record series is located. Provide additional information on other locations.

14. Frequency of Use

Record the frequency of use of record series. If parts of the record series have variable use record additional information on the back of the worksheet. Information provided in this section supports the development of a records retentions and disposition schedule.

15. Volume

Record the volume of the files or records in linear feet. Provide additional information on other measurements if necessary.

16. ATIPP Exceptions

It is important to identify whether the records contain information that may be excluded from access under the [Access to Information and Protection of Privacy Act](#), through either mandatory or discretionary exceptions. This effort may:

- Facilitate processing of ATIPP requests; and
- Impact conditions under which the records may be transferred to The Rooms Provincial Archives Division (TRPAD).

Identification of potential ATIPP exemptions should be done in consultation with the organization's ATIPP Coordinator.

Other Exceptions such as Provincial Regulations or Acts that prevail over ATIPP should also be listed, as outlined in [Newfoundland and Labrador Regulation 11/07](#).

If the record series contains records from Federal sources, *PIPEDA (Personal Information Protection and Electronic Document Act)* and/or other Federal privacy legislation may apply. The applicable legislation must be identified.

Appendix B: Records Inventory Worksheet

[Records and Information Inventory \(Excel Sheet\)](#)

[Records and Information Inventory Worksheet \(MS Word\)](#)



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – CLASSIFICATION PLAN DEVELOPMENT FOR OPERATIONAL RECORDS

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of Information Management programs. Guidelines generally clarify what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management
Approval Date	
Review Date	2015 03 24
OCIO TRIM Number	DOC03307/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	Corporate Records and Information Management Standard (C-RIMS)
Related Guidelines	Classification Plan Implementation Guideline Records and Information Inventory Guideline

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch	
	(name) (signature) (date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview	4
2.0	Scope.....	4
3.0	Recommended Approach.....	4
3.1	Introduction.....	4
3.2	Planning.....	5
3.2.1	Strategy.....	6
3.2.2	Communications Plan	6
3.2.3	Staff Training.....	6
3.2.4	Work Schedule.....	6
3.2.5	Monitoring and Updating Plan.....	6
3.3	Research and Analysis.....	6
3.3.1	Preliminary Research.....	6
3.3.2	Interviewing	7
3.3.3	Interview Questions.....	7
3.3.4	Scheduling Interviews	8
3.3.5	Compiling Results from Interviews.....	8
3.3.6	Completing Analysis.....	8
3.4	Building a Classification Plan	8
3.4.1	Classification Hierarchical Structure	8
3.4.2	Function	9
3.4.4	Secondary	9
3.4.5	File or Folder Level	10
3.4.6	Scope Notes.....	10
3.4.7	Arrangement and Classification Numbers	10
3.4.8	Completing the Classification Plan Template	11
4.0	Glossary	12
4.1	Definitions.....	12
4.2	Acronyms.....	12
5.0	References.....	13
6.0	Revision History	13
	Appendix A: Classification Interview Data Form	14

Guideline – Classification Plan Development for Operational Records

Appendix B: Interview Schedule for Classification Plan Project17
Appendix C: Classification Structure Template18

CLASSIFICATION PLAN DEVELOPMENT FOR OPERATIONAL RECORDS

GUIDELINE

1.0 Overview

This guideline outlines the activities necessary to develop a classification plan for operational records. Operational records are records that reflect the unique mandate of their creators. Records of programs, projects, and service delivery are examples of operational records. This guideline includes information and recommendations on planning and organizing for development; researching and gathering information; analyzing information gathered; structuring classification information; and preparing the classification plan for use.

Its purpose is:

- To provide a guideline for Government departments to develop a classification plan for operational records that complements existing standards including the Corporate Records and Information Management Standard (C-RIMS); and
- To ensure that a department's classification plan accurately represents the department's mandated functions and that it is easily used to support access to government records and information.

2.0 Scope

This Guideline applies to or may be used by all public bodies, as defined in the [Management of Information Act](#). Reference to department in this Guideline can be understood to include any public body.

3.0 Recommended Approach

3.1 Introduction

The purpose of a classification plan is to provide direction on how to systematically identify and categorize records and information created, received, processed and used by departments in a standardized manner. It is designed to capture the business functions of a department and establish rules around categorizing records created in the performance of these functions.

The information in a classification plan:

- Identifies the government records and information of the department;
- Provides a method to organize the use and storage of paper and electronic records and information;
- Shows record relationships necessary for supporting their authenticity;

- Provides [metadata](#) about the department's record and information assets;
- Organizes records and information to provide better access; and
- Aids a department in responding to Access to Information requests and legal discovery requirements.

Before undertaking development of a classification plan, a department should complete an inventory of its records, in all formats, to understand the types and nature of the records and information it creates, collects and manages. For further information about the inventory process, see OCIO Guideline *Records and Information Inventory*. The classification plan should be the second initiative a department should undertake and it should be followed by the creation of a records retention schedule. Corporate records (sometimes also known as Administrative Records) can be classified using [C-RIMS](#).

The scope of the classification plan is to identify and organize the records and information assets of the entire department down to the file level. Classification plans follow a hierarchy that includes a minimum of three to a maximum of five levels in its structure. Specialized file plans for records series may be further developed depending on the nature of the records.

Classification Plan Development tasks include:

- **Planning** - devising a plan for getting organized and overseeing the activities and processes involved in the project;
- **Research and Analysis** - conducting preliminary research and drafting a preliminary functional analysis; interviewing stakeholders to confirm and update analysis; collecting and compiling data; analyzing and organizing information; and completing functional analysis.
- **Building the Classification Plan** – putting information into classification hierarchical structure; drafting classification structure and compiling scope notes; getting feedback from stakeholders; completing the classification plan; obtaining approval from management; and preparing the classification plan for use.

The final classification plan is maintained as part of the department's records filed under C-RIMS classification # 08-01-42: *Information Management and Protection, Classification and Retention, Classification Plan*.

3.2 Planning

Creation of a records classification plan schedule should be treated and managed as a project, with project plans, resource allocation and timelines all managed by an individual who is accountable for the outcome. The department should develop a project plan that outlines the effort and resources necessary to complete the classification plan development. The project plan should contain the purpose and objectives of a classification plan; a strategy outlining the scope of the project and how it is being done; a communications plan; a list of project staff; staff training; and the work schedule.

Prior to developing a classification plan, a strategy needs to be developed and approval sought within the department. Success of the classification plan is dependent upon executive support and knowledge transfer from staff already using and working with the records. Communicating the strategy is essential to garnering cooperation of staff during the project.

3.2.1 Strategy

Identify the scope of the classification plan and a list of stakeholders, and include which business units will be interviewed. Consult with branches and divisions, if necessary, to determine what will work best for their specific business units. Seek the assistance of program staff that have specialized knowledge of their business functions, activities and information needs. Review the department's records inventory to understand the content required in the classification plan. In addition, identify who will be the final authority for approving the classification plan.

3.2.2 Communications Plan

When the strategy is complete and has Executive approval, communicate it to Executive and staff who will be involved in the classification plan development. This includes a presentation to the Executive, orientation and training to staff involved in the project, and a wrap-up or follow-up presentation to either or both reporting on the project and findings. The department's Executive should receive a presentation communicating the processes involved in the classification plan development, the role of staff and the projected work schedules so that they can communicate their support to staff to garner their cooperation.

3.2.3 Staff Training

Conduct workshop(s) to orientate selected staff involved in the project about the method and types of information being gathered. Train staff to use templates. Interviewees might require a one-sheet orientation about the project, classification and types of information needed from staff.

3.2.4 Work Schedule

Schedule the order of Divisions that will be interviewed and consult with Division supervisors to ensure that times selected are appropriate and that Division deadlines will not interfere with completing the project. Establish time-lines and completion dates. Adjust work schedule as the project proceeds.

3.2.5 Monitoring and Updating Plan

Monitor project time-lines and update the project plan as the classification plan proceeds. Timelines are likely to be affected due to the availability of staff and response to review requests. Adjust the project plan and report to Executive regularly about progress and any project risks or slippage in timelines.

3.3 Research and Analysis

3.3.1 Preliminary Research

Preliminary research is best gathered from the following sources: departmental organizational charts, legislation, regulations, policies, annual reports and strategic plans. For corporate functions, those functions common across government, it may be necessary to consult government-wide policies and processes. For instance, Government's Corporate Records and Information Management Standard ([C-RIMS](#)) or the Government policy on policy development provides information on the function and activities involved in formulating, establishing and reviewing Government policy.

Preliminary research provides background and insight into the organization, functions and business culture of the department, and is necessary for understanding how records and information should be organized and categorized. This information will provide context for

examining the department's information requirements and relationships within the department, the Government of Newfoundland and Labrador and the department's stakeholder community. Information gathered can be used in future Information Management processes such as in assessing the value of records and information and in developing a Records Retention and Disposal Schedule ([RRDS](#)).

When conducting preliminary research:

- Identify the main functions, sub-functions and activities of the department and assemble information in a hierarchical fashion to show their relationships. Departments, agencies, boards and commissions are mandated to perform specific functions and their records are usually arranged along functional lines of business.
- Identify stakeholders and gather contact information to be used for scheduling interviews and consultations.
- Determine the gaps in your research and form questions to be answered through further research. Also, examine the department's records inventory for records series, department files and file lists; consult former classification plans should they exist, and classifications for the same department or functions from other jurisdictions.
- Research the names and subjects commonly used and related to the department's functions. This will provide additional insight into the information needs of the creators and users of department records and information. Sources that provide this information include the records inventory, former classifications, individual records series and the files themselves. It is important to note that the terminology and language that the department uses should be included in building your classification plan in order for it to be relevant to users.

After the preliminary research has been completed, draft a preliminary functional analysis outlining the functions, sub-functions, activities and records identified in your findings. This outline becomes the foundation of the classification plan and indicates the gaps in your information gathering. Seek out additional sources to confirm and update your research. Scheduling and conducting consultations and interviews with key stakeholders within the department is the next step in developing a department's classification plan.

3.3.2 Interviewing Stakeholders

Stakeholders in the department will confirm the information you have assembled about the functions and activities they perform to do their work; update your findings; identify and incorporate new initiatives; and give insight into the records and information they create, receive and use. Interviews provide an opportunity to communicate about the project, respond to questions, and get feedback from creators and users about their records and information.

3.3.3 Interview Questions

A set of interview questions that can be adapted for use is provided in [Appendix A](#). These questions are the minimum that are necessary to gather information for developing a records classification plan. Additional questions may be included for collecting specialized information on a function or topic. The interview might also be expanded to include questions on records and information retention and value in preparation for the development of a [RRDS](#).

Depending on the culture of your organization, the questions can be sent ahead of the interview to prepare the interviewee. Some Managers may request the interview questions

and determine who would be best to be interviewed. It would be advisable to have two people conducting group interviews, one to ask questions and the other to take notes.

3.3.4 Scheduling Interviews

It is generally recommended to schedule management interviews first and separate from the other members of the business unit. Consult with management about which staff within the business unit should be interviewed to add detailed information about their business unit or have the most knowledge about its operations. Keep track of interviews; see a scheduling template in [Appendix B](#).

Interviews typically take one hour to conduct. However, schedule an extra half-hour between interviews to accommodate going over-time and to allow for a break to review your notes while interviews are still fresh. It is best to not schedule more than three interviews per day.

When setting up interviews inform interviewees of the duration of meetings and meeting location. It is advisable to request any functional or business process management charts outlining their business processes, file lists (physical and/or electronic), lists of acronyms, names of committees or working groups, and other documentation they deem to be useful to the interview or project.

3.3.5 Compiling Results from Interviews

Interview notes should be compiled as quickly as possible after the interview. The longer the data remains in its raw form the greater the likelihood of losing context for comments and forgetting shorthand notations used during interviews.

Assemble the information from interview responses following the structure of your preliminary research. The responses will add to the functional analysis of information already prepared from your preliminary research. Remember the purpose of the interviews is to confirm your research; supply new information where there are gaps, and brings it up to date with current information.

3.3.6 Completing Analysis

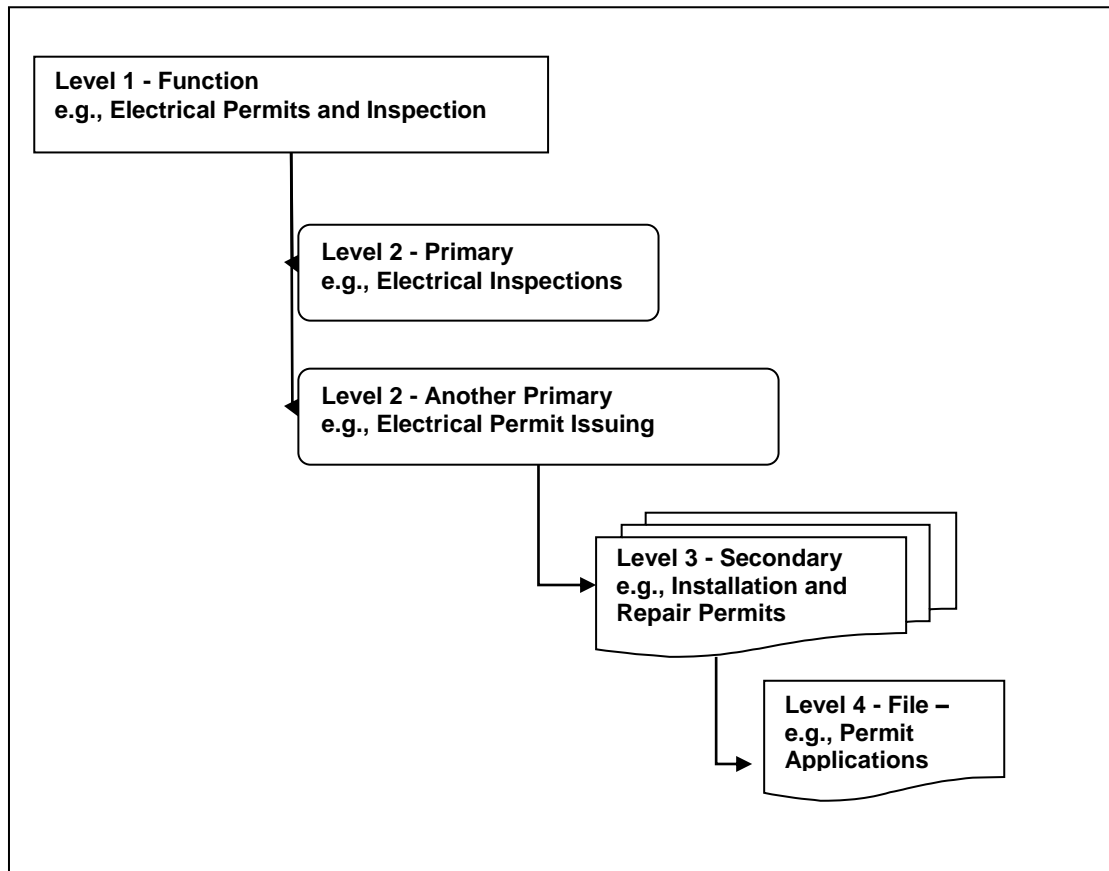
The completed functional analysis forms the foundation of a department's classification plan for operational records. It should include a hierarchical structure going from the general to the specific, relating functions, sub-functions and activities. It should also contain information defining what they are, how they are related and what type of information and records they contain. It is important to seek confirmation of the functional analysis from senior management before proceeding to building the classification plan.

3.4 Building a Classification Plan

3.4.1 Classification Hierarchical Structure

A hierarchical classification plan organizes records in a fashion that makes it easier to manage them through their life-cycle. Classification plans for operational records capture business functions relevant to a department, rather than subjects, the labels used to describe each level of the hierarchy will be different.

The hierarchical structure of the classification plan is three-tiered, going from the general to the specific, followed by individual containers or folders at the "file level" as the fourth level shown on the following page.



3.4.2 Function

The function is at the highest level on the classification plan and clusters together the next level of sub-functions and activities relating to that function. It represents a grouping of primary activities required to meet a particular mandate. For example, *Electrical Inspection* and *Electrical Permit Issuing* are sub-functions of *Electrical Permits and Inspection* and therefore are identified as separate primaries grouped under this function.

3.4.3 Primary

The primary is the next level and represents a grouping of secondary functions and activities that support the function it is attached to at the higher level. For example, the activities of receiving permit applications, review and approval by the Chief Electrical Inspector and the issuing of permits for electrical work in installation and repairs and electrical maintenance that support the primary *Electrical Permit Issuing* would form secondaries under this primary.

3.4.4 Secondary

The secondary is the next level and represents groupings of activities performed and some record series that support the higher level. We recommend using two types of secondaries: common and function specific secondaries. Common secondaries are those activities and record series commonly listed under each primary (e.g., *Working Groups*). Function specific secondaries are specialized types of activities and records series that are unique to that primary (e.g., *Installation and Repair Permits* under the Primary called *Electrical Permit Issuing*).

3.4.5 File or Folder Level

The file or folder is the lowest, most specific level of the classification plan, where the document (or information object) exists. It represents a container or “folder” of documents and information objects. For example, under the secondary *Installation and Repair Permits* are likely to have containers or files by name of applicant and/or permit number that includes permit applications, specifications of electrical work, additional plans or specs depending on the activity, approvals, permits, declines, and appeals that are necessary to organize various documents.

3.4.6 Scope Notes

Scope notes provide users with enough information to assist them in making the correct decision for identifying and capturing their records. This information is also important when developing an **RRDS**. Descriptions should be consistent in the organization of information being communicated. Each level refers to the next level in that it describes the groupings at the next lower level.

The description should contain a statement that includes the following types of information: 1) a definition of the function, primary or secondary; 2) a summary of the primaries or secondaries or records series beneath that level in the hierarchy; and 3) the types of information and records found in that specific classification. As you descend the level, additional information may be included (e.g., specific filing arrangements or a cross-reference to another classification).

Scope Notes Example
<p>Level 1 – Function Scope Notes</p> <p><i>Electrical Permits and Inspection</i></p> <p>The Electrical Permits and Inspection function provides a means to ensure public safety through regulation of electrical work being carried out by certified electricians and registered contractors. The Chief Electrical Inspector reviews applications, approves and issues electrical permits allowing electrical work to be carried out and conducts inspections of contractors' electrical work as defined in <i>the Public Safety Act</i> , snl1996 c.p-41.01 and Electrical Regulations nlr120/96.</p>
<p>Level 2 - Primary Scope Notes</p> <p><i>Electrical Permit Issuing</i></p> <p>Chief Electrical Inspector review and approval of permit applications that must be issued before installation or repair of any electrical equipment commences. The primary includes the issuance of two different permits: one for electrical installation and repair and the other for electrical maintenance.</p>
<p>Level 3 - Secondary Scope Notes</p> <p><i>Installation and Repair Permits</i></p> <p>Use for application submissions for electrical installation and repair permits for both single and non-single dwellings. Information includes permit applications, specifications of electrical work, building plans, approvals, permits, declines, and appeals. Arranged by applicant name and permit number.</p>

3.4.7 Arrangement and Classification Numbers

It is recommended that whenever possible the arrangement of each level within the hierarchy follow alphabetical order to facilitate browsing and filing.

A common method of numbering and one that is used widely in the Government is the block numeric system. Each level in the classification hierarchy is assigned a number resulting in a string of numbers that indicate how the records are tied to the main function. The function number is at the beginning followed in order by the primary, secondary and file numbers. For example, 400-20-20 is the classification number which represents Electrical Permits and Inspection (400) – Electrical Permit Issuing (20) – Installation and Repair Permits (20). The numbering system relates to specific categories of records.

When assigning numbers it is advisable to leave reasonable sized gaps to allow for additional functions, primaries and secondaries. The numbers assigned between gaps depend on the specific organization or business function. A business function that has been static for many years and not likely to change may not require large gaps; however, a function that is new or always changing will require larger gaps in order to support future changes. (e.g., in the example, the 1st level should be separated by hundreds and tens; the 2nd level separated by tens; and the 3rd level by tens.)

Numbering for secondaries is usually from 00-99. Usually the numbers from 00-14 are reserved for common secondaries.

Numbering for file units is discretionary to each records series although the number 1 should always be assigned as 01 or 001 to ensure proper filing order within an electronic environment.

3.4.8 Completing the Classification Plan Template

Classification plans should be compiled in a spreadsheet format in order to control the hierarchical structure and facilitate migration into an automated system, such as TRIM. A classification template has been compiled to assist departments in the development of departmental classifications. This template includes worksheets for classification structure hierarchy, C-RIMS, Operational Classification Plan, and common secondaries. See [Appendix C](#).

4.0 Glossary

4.1 Definitions

[Active Record](#)

[Classification Plan](#)

[Corporate Records](#)

[Corporate Records and Information Management \(C-RIMS\)](#)

[Government Record](#)

[Inventory](#)

[Metadata](#)

[Operational Records](#)

[Record](#)

[Record Series](#)

[Stakeholders](#)

[TRIM](#)

4.2 Acronyms

RRDS	Records and Retention Disposal Schedule
C-RIMS	Corporate Records and Information System

5.0 References

[Management of Information Act](#)

[Information Management and Protection Policy, TBM 2009-335](#)

[Government of Newfoundland and Labrador Corporate Records Information Management Standard I \(C-RIMS\) Manual](#)

ISO/TR 15489-2: 2001 - Information and Documentation - Records Management - Part 2: Guidelines

[DIRKS: A Strategic Approach to Managing Business Information \(DIRKS Manual\).](#)

6.0 Revision History

Date Reviewed	Reviewed By
2010-11-05	Access to Information and Protection of Privacy (ATIPP) Office
2010-11-22	Information Management Standards Board (IMSB)
2010-12-06	Iris Power, Director of Information Management Services
2011-01-07	Shelley Smith, Executive Director Information Management
2011-01-26	Government Records Committee (GRC)
2015-03-24	Bun Power, IM Consultant, IM Services

Appendix A: Classification Interview Data Form

Name of Interviewee (Last Name, First Name):	Date Interviewed (yyyy-mm-dd):
Program/Services Name:	

Questions	Reply to Questions
1. Major Functions or Activities	
1.1 What is the Mandate or purpose or Service?	
1.2 What basic activities are performed?	
1.3 Is the program or service centralized or decentralized?	
1.4 If decentralized, is it managed at a regional or district level?	
1.5 When did the program or service start?	
1.6 Was it part of another department previously? If yes, what department?	
2 Changes to Major Functions/Activities	
2.1 Have there been any major changes recently? Are any planned? What are the changes? Are they now obsolete?	
2.2 Are there any changes proposed to the enabling or programs specific legislation?	
3 Legislation/Policies/Procedure	
3.1 What legislation, regulation, policy or procedures guide your work? Can you make them available to our project?	
4 Record Series Information	
4.1 Briefly describe activities performed and identify associated records series.	
4.2 Who keeps the master records series?	

4.3	What media is the master or official record stored in?
4.4	What copies of the records are made and where are they?
4.5	What copies are stored in different media formats?
4.6	Are there issues related to the physical characteristics and storage of the records?
4.7	What is the growth rate of these records?
4.8	How are records created?
4.9	How are records organized?
4.10	Are there any plans to convert the records to another media?
5 Interrelationships/Partnerships with other Government Jurisdictions, GNL Organizations, Local Government, Non-Government Organizations	
5.1	What other organizations (government or private) are affected by the activities of the program or services? What interaction is there with these organizations?
5.2	Are there records that are created by government and then transferred to non-government business?
5.3	Are there records collected in non-government organizations performing government business.
6 Electronic Formats/Systems in Use	
6.1	What electronic information systems exist? Are electronic systems used to create records or to store or both?
7 Access/ Restrictions/PIB	

7.1 Are there Personal Information Banks being maintained and records series that may be subject to the exceptions to disclosure in ATIPP?	
7.2 What access restrictions apply to records now or in the past?	
8 Business Value	
8.1 How long will the record be of business value?	
9 Frequency of Use and Old Stuff	
9.1 When can the records be considered completed or closed?	
9.2 How long will the record be of business value?	
9.3 How often is it required after closure? How long and for what purpose?	
9.4 Do records need to be on-site for audit purposes or can audit take place offsite?	
9.5 Do you feel these records could be destroyed at the end of their life cycle? Why or why not? Is there historical value? Is there potential for research value?	

Appendix B: Interview Schedule for Classification Plan Project



S:\Information
Management\Educati

Appendix C: Classification Structure Template



S:\Information
Management\Educati



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – RECORDS CLASSIFICATION PLAN IMPLEMENTATION

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management
Approval Date	
Review Date	2015 03 10
OCIO TRIM Number	DOC03308/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	
Related Directives	
Related Standards	
Related Guidelines	Disposal of Records and Information Guideline Records and Information Inventory Guideline

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch	
	(name) (signature) (date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

1.0	Overview.....	3
2.0	Scope	3
3.0	Assumptions	3
4.0	Overview.....	4
4.1	Project Initiation.....	4
4.1.1	Project Kick Off.....	5
4.2	Project Planning	6
4.2.1	Scope Definition.....	6
4.2.2	Roles and Responsibilities	7
4.2.3	Document Project Plan	7
4.3	Communications and Change Management.....	7
4.3.1	Communications Plan.....	7
4.3.2	Records Classification Plan Project Working Group	8
4.4	Program Documentation	9
5.0	Implementation	9
5.1.1	Inventory	10
5.1.2	Training.....	10
5.1.3	Backlog Elimination	10
5.1.4	Reclassification.....	11
5.1.5	Monitoring and Controlling.....	11
5.1.6	Transfer to Operations.....	11
5.2	Post-Implementation Review	12
6.0	Glossary.....	13
6.1	Definitions.....	13
6.2	Acronyms	13
7.0	References	13
8.0	Revision History.....	14

RECORDS CLASSIFICATION PLAN IMPLEMENTATION

GUIDELINE

1.0 Overview

The *Records Classification Plan Implementation Guideline* (hereafter referred to as the *Guideline*) provides public bodies with an approach to implementing a records classification plan. A records classification plan identifies and organizes records by arranging the records generated by business activities into categories according to standard conventions, methods and procedural rules. Implementing a records classification plan will:

- Improve the ability to easily access all relevant records to complete business transactions;
- Support compliance with legal and operational requirements related to Information management (IM);
- Provide an overall view of a public body's information assets and their interrelationships;
- Provide day-to-day guidance to employees on how to process/access information;
- Provide a critical path for locating information for retrieval, maintenance, retention and disposal, litigation discovery, requests processed through the *Access to Information and Protection of Privacy Act* (ATIPPA) and legal holds.

2.0 Scope

This *Guideline* applies to or may be used by all public bodies (hereafter referred to as *department* in this document) as defined in the *Management of Information Act*. This guideline has been developed to provide direction to:

- Executives and senior management who are accountable for the operation of an information management program within their department;
- Departmental IM resources responsible for the implementation and maintenance of classification plans.

3.0 Assumptions

This *Guideline* has been developed with the assumption that:

- A records classification plan structure has been approved for use within the department.
- Business rules required to support the use of the records classification plan, including naming conventions, labeling practices, etc. are in use within the department.

4.0 Overview

A comprehensive Records Classification Plan is a critical tool in a department's IM program. If information is not organized and accessible, it cannot be managed. The fact that almost all employees will play a role in classification, combined with the need for consistency in the way information is handled, are two critical challenges. The project plan detailed in this section incorporates the planning, communications and change management required to successfully implement the records classification plan and incorporate it into ongoing IM operations. It is meant to be used as a starting point for success, and can be augmented to accommodate a department's specific requirements.

4.1 Project Initiation

Implementing a records classification plan is a significant effort even for the smallest organization. This is why it needs to be recognized as a project in its own right that will require time, planning and resources. At the initiation point there must be a minimum of two resources identified:

Project Sponsor: The project will require a sponsor who will have final decision making authority on behalf of the department. This should be at an executive or senior management level. The sponsor will:

- Provide direction on the scope, timeline and priorities of the project;
- Allocate resources to work on the project;
- Play a critical role in communicating to employees at all levels their required involvement;
- Resolve issues as they arise.

Project Manager: The project manager will be responsible for coordinating the planning and implementation of the project. Choosing a project manager with a strong IM background is essential. The project manager will:

- Implement planning and management for the project;
- Communicate and be responsible for necessary change management plans and activities;
- Provide regular project reports to the Project Sponsor and any other designated individuals or committees;
- Coordinate Services required to carry out the project, such as procuring supplies and storage as required as well as identifying personnel resources needed for project success.
- Oversee the project implementation, identifying and resolving issues during the course of the project.

The first step in moving the project forward is a high-level planning session between the project sponsor and project manager. This will result in:

- Identifying the business need or driver for the project;
- Documenting decisions/information already known about the project (e.g., priorities, scope, timeline, issues, etc.);
- Identifying departmental project management standards/resources that must be incorporated into the project;

- Identifying resources to be included in the project kick-off meeting;
- Defining agenda for the Project Kick-off meeting.

4.1.1 Project Kick Off

The project kick off engages all the resources that will play a critical role in the project implementation. These resources likely fall into two categories. First there are subject matter experts (e.g. IM resources), who have knowledge of the organization that is required to plan and implement the project. Second there are managers of priority areas that need to make available resources to implement the project (e.g., Corporate Operations, priority program areas, etc.). The Agenda for this meeting may include:

- *Overview of Departmental Records Classification* – Provide a description of the records classification plan, who was responsible for its development, existing implementations within the department, etc.
- *Project objectives* – These will likely have been set by the sponsor and may be at a high-level at this time and may be modified following the kick-off session.
- *Define the Scope of Project* – This will be largely dependant on where the group sees the greatest need for the records classification plan to be implemented as a first step. For example, some departments choose to focus on classifying their physical records before moving into the classification of their electronic records. These are important decisions, as they will impact resources, timeline, training materials, etc.
- *Identify Potential Conflicts* – Are there any known activities such as busy operational times (e.g., end of fiscal year, beginning of busy program period, etc.) or ongoing projects that will impact a business unit's ability to participate in the project?
- *Timeline* – Set realistic goals around the timeline for the project at a high-level. Detailed estimates can be made in the project planning process.
- *Quick Wins* – Are there any known areas that can be used as quick wins – meaning that there is consensus amongst the project team that the implementation of the records classification plan in this particular area will be recognized as successful? The Project Manager may wish to schedule this area earlier in the planning process as a motivator for other areas, and to maintain support/momentum for the project.
- *Transferring to Operations* – Discuss the resources required to support the ongoing use and maintenance of the records classification plan following implementation.
- *Roles and Responsibilities* – Define roles and responsibilities for the project team – Including the project sponsor, project manager and any known resources.
 - *Project Sponsor* – Executive or Senior manager accountable for the project.
 - *Project Manager* – Resource responsible for the planning and delivery of the project and for project communications/change management.
 - *Business Unit Lead*: Contact for each business unit to support the project.
 - *Information Management*: Departmental IM resources.
 - *Technical Resource*: Depending on the scope of the project there may need to be resources identified to act as technical consultants or as liaison with the Office of the Chief Information Officer on the management of electronic records.
- *Financial Resources* – Define the financial resources that will be available/required for the project. Understanding constraints will have an impact on the scope/timeline of the project.
- *Physical Resources* – Identify any physical resources that are known to be required (e.g., new filing area, storage space, shelving, filing supplies, etc.). Ensure that this is validated with each business unit.
- *Communications Planning* – Ongoing communications are critical to the success of the project. Ensure that roles for communications related to the project are clearly

defined and ensure that appropriate resources are engaged if required (e.g. departmental or corporate communications employees).

- *Reporting Requirements* – Identify scope, frequency and participants in reporting on project activities.
- *Next Steps* – Next steps will likely include identifying the next series of meeting required to ensure that there is support for the project within each business unit.

The goal of this meeting is to ensure that information about the project is known and that potential issues/risks are mitigated. Incorporate communicating back to this group regularly as a part of the communications plan. This group will be the project steering committee. Following the review and approval of the minutes, the planning effort can begin.

4.2 Project Planning

All projects must have a beginning, middle and an end. There is a risk with records classification projects that the effort will drag on indefinitely if constraints are not placed on activities. The project plan is designed to keep the project on track. At a minimum, it should:

- Define project scope timeline and constraints;
- Identify and sequence activities required to complete the project;
- Identify and allocate resources;
- Reinforce communications through the project;
- Ensure efficient reporting of project activities/milestones.

4.2.1 Scope Definition

Having a clear definition of what is in and out of scope for the project is critical. This information is needed to guide decisions about the project, including the timeline, resources required and sequence of activities. All of the information holdings may include:

- Paper records stored on site within business units, file rooms and registries as well as at personal workstations;
- Paper records stored at offsite locations including third party storage vendors, the Provincial Records Centre, government buildings, etc.;
- Electronic records stored on the shared or network drive;
- Electronic records stored within personal network drives and e-mail accounts;
- Electronic records stored within business applications.

Work with the project team to identify all potential storage locations for departmental information and then determine which locations will be included in the records classification plan project. Some departments, for example, choose to focus on paper records first and then move to other locations such as the network shared drive. Understanding the business driver for the project (e.g., inability to respond quickly enough to requests for electronic information, costs of storing paper records in commercial storage facilities, etc.) will assist you in making decisions about the scope included in each phase of the project.

4.2.2 Roles and Responsibilities

Roles need to be defined for both the project designed to implement the records classification plan and the ongoing monitoring and development of it (see Section 4.1.1). Roles for the project include:

- Project Sponsor
- Project Manager
- Information Management
- Business Unit Leads
- Technical Resources

Support for the records classification plan following the completion of the project is critical. A records classification plan is based on departmental business processes. Over time, these processes are likely to change. For example, the way the information flows may be impacted when new technologies are introduced to the work environment, new programs or projects are implemented, or legislation is introduced or amended. These changes need to be reflected in the records classification plan.

A periodic review of the classification plan should be completed by the information management team (e.g. annual). The senior IM Manager or the IM Director may wish to establish an on-going IM Steering Committee or focus group to provide advice and identify issues and requirements in the implementation of the department's IM program overall, including any necessary changes to the records classification plan.

4.2.3 Document Project Plan

Given what is known about the department, the state of the existing records classification plan and the scope of the project, the next step to planning the project is to identify all the tasks that need to be completed to coordinate the overall project and to accommodate business unit specific requirements. Identify and sequence all tasks in the project plan and identify the appropriate resource responsible.

The project plan needs to be monitored on a regular basis to ensure that all components including timeline, resources, etc. are adjusted when changes occur that have an impact on the project. Most project managers find it helpful to retain a document that includes the project tasks in sequence, target dates to begin/complete the task, resources assigned and work effort required. It may be useful to use project management software such as Microsoft Project to assist in this effort and in keeping the project on track.

4.3 Communications and Change Management

The use of a new classification plan may change the way that employees perform selected functions. The level of change will depend upon the variance between current and proposed records classification practices. Having targeted, consistent and timely communications and change management support will ease the transition of employees from current practices to new responsibilities. A good communications plan will assist with the transition of departmental employees while a dedicated working group will assist employees who will be more hands on through the implementation and possible ongoing operation of the records classification plan.

4.3.1 Communications Plan

Communicating the records classification plan implementation project is critical to its success. The goal of a well defined communications plan is to:

- Identify all persons or groups, often referred to as stakeholders, which are impacted or may impact the success of the project. It is important that the stakeholders identified in the roles and responsibilities above understand what is required of them to make the project a success. Furthermore, when people are introduced to the project early, and given time to participate, address concerns, etc. they see themselves as a part of the project. Building a sense of ownership of the project across the department is important, as employees are more likely to get engaged in the project and want to see it succeed if it is something in which they feel a sense of ownership.
- Define the key messages that each stakeholder group needs to receive and when. It is also important that the messages are delivered in an appropriate manner to each group. For example, having the Deputy or Executive take the lead in communicating the project across the department gives the project a level of priority that is unlikely to be assigned when the message is delivered from someone outside of the senior executive team.
- Identify communication venues that can be used to disseminate information about the project (e.g. regular management meetings, annual departmental session, weekly team meetings).
- Identify communication tools that can be used to communicate the project and maintain awareness (e.g. web site, e-mail from deputies, monthly reports to staff, departmental intranet or newsletter).
- Define a sequence of communications that are required to support the project that can be incorporated into the overall project plan (e.g. Week 1 – Memo from Deputy to all staff about the project, Week 5 – Communicate a Milestone).

Incorporate all communications into the project plan to ensure that they occur at an appropriate time.

4.3.2 Records Classification Plan Project Working Group

The implementation of the records classification plan may initiate a group of employees from program areas, in addition to the project team outlined above, who will assume a role in supporting information management. One way to establish relationships with and between these resources is to form a records classification plan project working group. The purpose of this group is to disseminate and gather information, and to provide a support network for the business unit leads on the project team.

The working group will be comprised of departmental resources that have been identified by each business unit to lead the implementation of the records classification plan in their respective areas. It is likely that these employees will be in support roles whereby they already perform some information management related tasks such as filing, boxing and transferring records offsite, recalling records when required, ordering filing supplies, etc. Often these will be Administrative Assistants in the program areas of the department.

The success of the project and ongoing use of the records classification program is largely dependent on the ability of these key resources to provide information to the project team, and assist in the implementation. Initiating a working group to pull together these employees is a great way to establish relationships with the project team. It will also serve to expand the overall IM capacity of the department. Sessions with the working groups may include:

- Project Introduction, including their role
- IM 101 Workshop

- How to Use the Records Classification Plan
- Review/Validate Departmental Business Rules
- Prepare Business Unit Specific Documentation
- Knowledge Transfer

Incorporate all sessions into the project plan to ensure that they are scheduled at appropriate times.

4.4 Program Documentation

There are two types of documentation that may be required to get the project moving. These are corporate level documentation and business unit specific documentation.

Corporate level documentation is prepared by the project team in consultation with relevant stakeholders. This documentation is to be implemented for all business units. Corporate level documentation includes:

- *Business Rules* – Business rules relate to the handling and use of information and apply across the department. Business rules may include practices related to document or file naming conventions and terminology. In developing these department-specific rules, a department should ensure alignment with any existing Government-wide policies Standards and Guidelines that the department must use. These are available on the [OCIO Website](#).
- *Records Classification Plan* – The records classification plan needs to be in a format that is accessible to non-information management employees who may need to consult it. Review the records classification plan with the lead from each business unit to ensure that the components related to their business processes accurately, reflect the work performed, and that the language used will be acceptable and familiar to employees.
- *Job Aids* – Job aids are an important tool to support the implementation and ongoing use of the records classification plan. Job aids are typically quick references to act as reminders to employees. Sample quick references are available on the [OCIO Website](#).
- *Project Communications* – A set of documentation that communicates the project and can be used to support the implementation in multiple business units is essential. For example, presentations that provide an overview of the project, describe how to classify records, and outline how the ongoing program will work following the implementation, can be re-used by each business unit and ensure that the information given to all employees is consistent.

Information that is specific to the business processes of each business unit (e.g., application processing), that have specialized information handling requirements (e.g. confidential or personal information) should be identified. The relevant business unit lead will be responsible for the preparation of this material with the assistance of the information management team.

5.0 Implementation

The implementation of a records classification plan will be different for every department as each department has unique business needs and information flows. Each department will identify a scope and timeline for their project that will reflect these requirements. The

following is a suggested implementation that can be repeated for individual business units as required. Depending upon how the project has been structured and resources available, multiple business units can be scheduled for implementation at the same time. The level of effort required for each of the following steps will also vary depending on business needs:

- Inventory
- Training
- Backlog Elimination
- Reclassification
- Transfer to Operations
- Post-implementation Review

5.1.1 Inventory

An inventory is a detailed survey of the organization's records, including descriptions, scope, volume, frequency of use, method of organization and retention periods. It is used as the basis for developing a records management system. Completing an inventory is critical because unless a business unit knows its information holdings cannot readily manage them. See the OCIO's Guideline *Records and Information Inventory* for detailed instructions.

5.1.2 Training

Training on how to use the classification plan is required for any employees that are creating and storing information on behalf of the department. Each business unit will have identified an employee that will act as a business unit lead. This resource will assist in scheduling any training and act as the project contact. Employee training will include:

- Project overview
- Their role in the project and post-implementation operations
- The projected timeline for the project
- How to classify records using the records classification plan
- How to support employees in their business unit through the implementation and operations

5.1.3 Backlog Elimination

The goal of the records classification plan implementation is to establish the use of the records classification plan for the organization of departmental information. The required effort to complete this implementation will vary depending on the variance between existing practices and the records classification plan. The goal of the backlog elimination will be to remove records from the departmental holdings prior to the implementation of the records classification plan. This results in a reduction in the overall volume of records that will require reclassification. Backlog elimination focuses on the:

- Secure Destruction of Transitory Records;
- Identification of records which may be disposed of using One Time Disposal authorization by the Government Records Committee;

- Approval from the Government Records Committee to apply the Corporate Records and Information Management System (C-RIMS) for the destruction of corporate information per the C-RIMS retention periods; and
- Disposal of records under any existing Government Records Committee approved Records Retention and Disposal Schedules.

Use the *Guideline – Disposal of Records and Information* to eliminate the departmental backlog. The elimination of the backlog results in the retention of only those records that are active and must be retained and accessible to the business unit. This is the information that requires classification or reclassification using the records classification plan.

5.1.4 Reclassification

Reclassification involves the reorganization of records into the components identified in the records classification plan. The level of effort required to reclassify records varies depending upon the variance between existing practices and the records classification plan and the scope of the project (e.g., whole department or individual business units).

Steps to reclassify information may include:

- Analysis – Identify records;
- Information Mapping – Map Information to classification plan;
- Physical Preparation – Create required physical folders/labels; network folders; or folders and classification in a content management solution such as TRIM. Technical resources may be required for electronic data depending on the scope of the project;
- Transfer – Transfer information (paper or electronic) to the new classification location (e.g., paper folder, network folder, TRIM folder or classification); and
- Update Documentation – This may include the inventory, indices or other documentation maintained by the business unit or corporate IM staff to retain an up to date profile of information holdings.

5.1.5 Monitoring and Controlling

Following the immediate implementation it is important to assess how the records classification plan is working following implementation. Following implementation, complete an informal assessment of how the records classification plan is working. This may include a series of short interviews with targeted resources to determine:

- Validate project objectives;
- Determine if the records classification plan is working;
- Determine if there is information that is not accommodated in the records classification plan;
- Validate that roles and responsibilities are clearly understood; and
- Update project deliverables (if required).

5.1.6 Transfer to Operations

Transferring the records classification plan to operations means that the backlog of records has been eliminated and employees are now using the records classification plan to organize and retrieve information. Use of the records classification plan is a part of

ongoing operations. At this time it is important to reinforce the responsibilities earlier established (Section 4.2.2) to support the records classification plan. Activities include:

- Updating the records classification plan as required;
- Communicating changes to the records classification to employees and to departmental IM; and
- Orienting new employees on the use of the records classification plan.

5.2 Post-Implementation Review

A post-implementation review is an important phase of the project. This is to assist a department in measuring the effectiveness of the records classification plan and records system and to evaluate the records classification plan in order to remedy deficiencies. The records classification plan needs to be in use for a period of time to properly gauge effectiveness. Four to six months following completion of the project would be a good target. Responsibility for this activity will vary depending on the roles and responsibilities established for the project versus ongoing operations (Section 4.2.2). This review may include:

- Observation of how the system is working with the random checking of operations;
- Feedback from users through interviews and surveys.

6.0 Glossary

6.1 Definitions

[Classification Plan](#)

[Corporate Records](#)

[Life Cycle](#)

[Office of Primary Responsibility \(OPR\)](#)

[Operational Records](#)

6.2 Acronyms

C-RIMS	Corporate Records and Information Management Standard
ATTIPP	Access to Information and Protection of Privacy
IM	Information Management
GRC	Government Records Committee
OCIO	Office of the Chief Information Officer

7.0 References

[Management of Information Act](#)

[Information Management and Protection Policy, TBM 2009-335](#)

Guideline – Classification Plan Development for Operational Records

[CRIMS](#)

8.0 Revision History

Date Reviewed	Reviewed By
2010-11-19	Lori Collins, Coordinator Education and Awareness
2010-12-20	Iris Power, Director of Information Management Services
2010-12-21	Shelley Smith, Executive Director Information Management
2011-01-26	Information Management Standards Board (IMSB)
2011-02-24	Government Records Committee (GRC)
2015-03-10	Bun Power, IM Consultant, IM Services



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – DISPOSAL OF RECORDS

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of the information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015 03 23
OCIO TRIM Number	DOC03309/2011
Authorizing Directive <i>(Where applicable)</i>	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	Corporate Records and Information Management Standard
Related Guidelines	

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

- 1.0 Overview 1
- 2.0 Scope 1
- 3.0 Recommended Approach 1
 - 3.1 Introduction 1
 - 3.2 Identifying and Disposing of Different Types of Records 2
 - 3.2.1 Records 2
 - 3.2.2 Government Records 2
 - 3.2.3 Transitory Records 3
 - 3.2.4 Cabinet Records 4
 - 3.2.5 Publicly Released Documents 4
 - 3.2.6 Abandoned Records 4
 - 3.2.7 Active versus Semi-Active Records 4
 - 3.3 Implementing Disposal Authorities 5
 - 3.3.1 Records Retention and Disposal Schedules 5
 - 3.3.2 One-time Disposal 6
 - 3.3.3 The Disposal Process 6
 - 3.3.4 Variances in the Disposal Process 7
- 4.0 Executing Disposal 7
 - 4.1 Master Standing Offer Agreements 7
 - 4.2 Secure Destruction 8
 - 4.2.1 Paper/Microforms 8
 - 4.2.2 Electronic Records On the Shared/Network Drive 8
 - 4.2.3 Electronic Data 9
 - 4.3 Transfer of Records to The Rooms Provincial Archives Division 9
- 5.0 Glossary 9
 - 5.1 Definitions 9
 - 5.2 Acronyms 9
- 6.0 References 10
- 7.0 Revision History 10

DISPOSAL OF RECORDS AND INFORMATION

GUIDELINE

1.0 Overview

This *Disposal of Records and Information Guideline* (hereafter referred to as the *Guideline*) outlines requirements for the disposal of government records. Records disposal in the Government of Newfoundland and Labrador refers to authorized removal of records by means of destruction, transfer to The Rooms Provincial Archives Division (TRPAD) for permanent preservation, or transfer to another entity. Disposal of records can only be carried out in one of three ways: as part of implementing approved records retention and disposal schedules; as a result of a destruction request authorized by the Government Records Committee; or as an authorized transfer of records to another entity. The disposal of government records must be authorized by the Government Records Committee (GRC) as per the [Management of Information Act](#).

This *Guideline*:

- Outlines disposal requirements for different record types;
- Describes disposal authorities and how they are implemented; and
- Details disposal options including secure destruction, transfer of records to TRPAD for permanent preservation, and transfer to another entity.

2.0 Scope

This *Guideline* applies to or may be used by all public bodies (referred to as departments throughout this *Guideline*), as defined in [The Management of Information Act](#). Its audience includes employees responsible for the management and protection of records and information of public bodies.

3.0 Recommended Approach

3.1 Introduction

Disposal of records refers to the implementation of records retention, destruction or transfer decisions. These decisions are typically documented in government approved disposal authorities as part of a department's Information Management (IM) program. The [Management of Information Act](#) (Section 6) requires that all departments:

- Shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records;

- Will implement a system that provides for retention periods and disposal by either destruction, or transfer to the archives, in accordance with the guidelines and schedules established by the GRC;
- Shall ensure that the retention, disposal and removal of government records is carried out in accordance with the *Management of Information Act*.

Without a proper approach to dispose of records in a timely and legally authorized manner, a department may have to address:

- Inefficient use of resources, including:
 - Budget unnecessarily spent on storage space;
 - Time and resources wasted on inefficient search and retrieval;
 - Cost to process information requested by legal authorities or public access that is no longer necessary for the department's business and which could have been legally destroyed under an appropriate retention and disposal program.
- Legal action against the Government of Newfoundland and Labrador and/or its employees if information is disposed of without appropriate authorization.

3.2 Identifying and Disposing of Different Types of Records

Not all records have the same disposal requirements. Departments must identify and implement appropriate disposal requirements for different record types.

3.2.1 Records

The *Management of Information Act* defines a record as:

“A correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic.”

The broad definition of a record means that all government information, regardless of media must be managed in a secure and efficient manner including:

- E-mail messages sent and received by government employees
- Office records including MS Word documents, PowerPoint presentations, spreadsheets
- Physical records stored onsite at workstations, file rooms, etc.
- Boxes of records in offsite storage locations
- Database records in departmental business applications

3.2.2 Government Records

The *Management of Information Act* defines a government record as:

“A record created by or received by a public body in the conduct of its affairs and includes a Cabinet record, transitory record and an abandoned record.”

Legal disposal of government records must be completed in accordance with the *Management of Information Act* and with the approval of the GRC. The preferred method

of disposal is through the ongoing implementation of a Records Retention and Disposal Schedule (RRDS). This effort is required because these records may need to be retained for a legal reason, or may need to be transferred to TRPAD because they have been appraised as having enduring value.

Some examples of government records include:

- Completed application forms and receipts,
- Case files, client files, work orders or reports related to providing a service,
- Recommendations and decisions including relevant supporting material such as briefing notes,
- E-mails documenting decisions or providing direction for action,
- Deliverables provided to the government by consultants or contractors,
- Data stored within information technology applications used to support operational functions, service delivery and decision making.

The disposal of government records must be documented. This documentation about records disposal should be retained by the department according to the retention periods and disposal requirements set out for records related to the information management function by the *Corporate Records and Information Management System (C-RIMS)*. The requirements and processes described in this guideline will assist departments in ensuring that their IM program disposes of government records appropriately.

3.2.3 Transitory Records

The *Management of Information Act* defines a transitory record as:

“A government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.”

Transitory records can be securely destroyed when no longer of operational value to the department. Authorization by the GRC is not required to dispose of transitory records. It is recommended that departments develop an internal process for the identification and disposal of transitory records as part of their overall IM Strategy. It is important to note that if they exist and are accessible, transitory records must be produced in the event of an audit, legal inquiry or ATIPP request. Timely disposal of transitory records is encouraged to minimize resources required for their storage and management. Some examples of transitory records include:

- Convenience copies of information retained for reference purposes,
- Copy of a report of a government record available in an alternate location and format,
- Drafts of records which reflect content that is included in the final version of the record or contain only minor edits to content or formatting changes,
- Supporting information used in the preparation of a subsequent record,
- Records not directly related to you or your office that do not require you to act,
- Transmittal or routing slips and opened envelopes.

The destruction of transitory records does not need to be recorded by the department; however an overall business rule or general approach to the destruction of transitory records should be documented. Transitory records may contain personal or confidential information. Secure destruction practices should be adhered to by departments when disposing of transitory records.

3.2.4 Cabinet Records

Cabinet records are among the most highly confidential records created in government. They have specific management requirements that must be adhered to by all departments. As per the *Management of Information Act*, these requirements are defined by Cabinet Secretariat. Questions regarding the management and disposal of Cabinet records should be directed to Cabinet Secretariat.

3.2.5 Publicly Released Documents

The Legislative Library is the official depository for the publicly released government documents of Newfoundland and Labrador. It is the Library's responsibility to preserve and make accessible these materials for long-term use and historical posterity regardless of their original format or storage medium. Publicly released documents include documents published by government and its agencies, and other documents such as agreements, letters, and press releases, which are publicly released or tabled in the House of Assembly by government departments, and other public bodies. Additional materials may be acquired at the discretion of the legislative librarian.

As per section 21.6 of The *Rooms Act*, copies of publicly released documents must be transferred to the Legislative Library. Departments should make this practice a regular course of business such that a copy is transferred immediately following its release. In the event that publicly released documents are discovered during the disposal process, departments are advised to verify with the Legislative Library whether copies of these materials have been received by the Library and have been incorporated into the existing collection.

3.2.6 Abandoned Records

The *Management of Information Act* provides a definition of abandoned records as follows:

“A government record to which ownership cannot be established and which has been determined to be an abandoned record by the Chief Information Officer (CIO).”

Incidence of truly abandoned records is rare. Records are usually able to be linked to a government process that can be traced back to an organizational unit responsible for it. Because the true value of abandoned records may initially be unknown, there may be significant effort required to dispose of abandoned records. The OCIO will work with departments on a case by case basis to determine an appropriate approach to the disposal of records deemed to be truly abandoned.

3.2.7 Active versus Semi-Active Records

Identifying whether records are active or semi-active is important. It is when records cease to be active that the disposal process begins. Active records are consulted frequently to support a department's operational requirements or business. They must be quickly available for reference. As a general rule, records accessed more than once a month are considered active. All records start out as being active. By organizing active records according to the disposal requirement (e.g., by calendar or fiscal year, project

number, etc.), it will be easier to identify and process records that are ready to be destroyed or transferred.

Departments are required to retain records to support both operational and legal requirements. A Department may need to retain records for legal reasons long after they have fulfilled their operational usefulness. Semi-active records (also sometimes referred to as inactive) are records that do not have to be readily available but which still need to be kept for the possibility of use or reference. Offsite storage, like the Provincial Records Centre or third party commercial storage locations provides a less expensive alternative for record storage.

An approved Records Retention and Disposal Schedule will help to ensure that records are transferred offsite when appropriate. It is divided into three parts: 1) the active period (ACT); 2) the semi-active period (SA); and 3) the method of disposal (DIS).

3.3 Implementing Disposal Authorities

A disposal authority provides the legal authorization to dispose of a government record. There are two types of disposal authorities used in the Government of Newfoundland and Labrador. These include:

- Records Retention and Disposal Schedule (RRDS)
- One Time Disposal (OTD) Submission

Understanding these disposal authorities; how/when they are used; and exceptions to the disposal process supports the operation of the IM program.

3.3.1 Records Retention and Disposal Schedules

The disposal of government records requires the authorization of the Government Records Committee. The recommended disposal authority for government records is a RRDS. A RRDS signifies a legal requirement on the part of a department. Departments may dispose of records as per the following:

- The *Corporate Records and Information Standard (C-RIMS)*, which is the standard used to dispose of government corporate or administrative records;
- Departmental RRDS for Operations Records. Please refer to the OCIO website for the latest version of the [RRDS](#) process.

Ongoing implementation of RRDS ensures appropriate disposal of records when they cease to be of operational or legal value. Disposal is either:

- Destroy: Records that have no operational or legal value to a department are destroyed; or
- Transfer to Archives: Custody of records of enduring historical or cultural value is transferred to TRPAD.
- Transfer of publicly released government documents to the Legislative Library: As per section 21.6 of *The Rooms Act*, copies of records produced by a department for general or limited distribution to the public must be transferred to the Legislative Library. Contact the Legislative Library prior to initiating transfer of materials. The Library will generally accept up to four copies of any one title/item not already in the collection.

- **Transfer to another entity:** Records are transferred to an entity outside of the entity that created them, as in the case of a business unit moving into a separate Crown Agency for example.

Disposal is documented and approved in the RRDS. Once a department has a RRDS approved, it is their responsibility to implement as part of the regular course of business.

3.3.2 One-time Disposal

A One Time Disposal (OTD) submission may be used to dispose of a backlog of inactive records. An OTD is not meant to be a replacement for the regular and consistent implementation of a RRDS. It may be used when records have resulted from an activity no longer in progress (e.g. organizational unit, service or function that no longer exists, or business function or project which was created to suit a specific purpose and had a specific lifespan). The process includes an inventory of the records, the volume of the records in question and the submission of a completed OTD Submission Form to the Government Records Committee. Information on OTD Submissions can be located on the OCIO Website in the [One Time Disposal](#) section.

3.3.3 The Disposal Process

Disposal of records is a key objective of all the tools/activities within a department's IM program. Each department will have to define their own processes. Typical steps include:

Step 1: Planning and Operations: Planning for records disposal within a department as a part of its ongoing operations is the best way to ensure that disposal occurs in a timely manner. The frequency with which records need to be disposed will vary depending on the nature of a department's business and the retention periods established by its records retention and disposal schedules. Some departments are heavily focused on the end of calendar or fiscal year, school year, etc. and can close files at that time. Others rely on the completion of programs or services to initiate disposal. Be familiar with the department's RRDS and schedule activities at appropriate intervals to initiate disposal. A records classification plan can be used to organize records according to disposal requirements. This makes it easier to identify and physically prepare records for disposal.

Using the RRDS and other IM tools such as the inventory, records classification plan, etc., identify the records that must be disposed of at this time. Identify records that have met their retention requirement and must now be either destroyed or transferred to TRPAD.

Step 2: Notify ATIPP Coordinator: The departmental ATIPP coordinator will be aware of ongoing ATIPP requests that may require the disposal of records to be placed on hold.

Step 3: Eliminate Transitory Records: Secure destruction of any transitory records eliminates unnecessary processing (e.g., creating folders, boxing and documenting records to prepare for transfer).

Step 4: Prepare Documentation: Whether you are destroying records or transferring them to TRPAD or another entity, sufficient information about the records should be captured to ensure the department retains a complete inventory of both the information that it holds and the information disposed. This includes:

- *Record Series/File Documentation:* The amount of documentation required to ensure accessibility varies depending on the nature of the department's business. For example, in the case of paper records, a box containing project or claim files may need a detailed list that includes the name or identifier for each file. Alternatively, a processing centre may be able to put a range of numbers/dates on a box and, because they file sequentially or by date, they are able to track the content of the box with that amount of information.

Departments are advised to develop their own forms that capture appropriate level of information to ensure that the content of the records in question are known. These forms should be consistently used by all employees responsible for the processing of records. Suggested content may include:

- Disposal Number
 - Record Series Title
 - Description of Records
 - Date or Date Range of Records
 - Quantity or Volume of Records
 - Date of Disposal
 - Witness/Authority
 - Organizational Unit (Department/Branch/Division)
- Transfer documentation: Documents are required to complete the transfer of records to either offsite storage or to TRPAD in Section 5 of this guideline *Executing Disposal*.

Step 5: Execute Disposal: Executing the disposal will vary depending on the nature of the disposal. The various options for disposal and the detailed requirements/processes are described in Section 5 of this guideline *Executing Disposal*.

Step 6: Retain/Update Documentation: C-RIMS includes requirements for retention and disposal of records related to a Department's IM program. Following the disposal of information, update any related departmental inventories, classification plans, finding aids, etc. to ensure accessibility of information. Copies of completed transfer lists and certificates of destruction are to be retained as per C-RIMS.

3.3.4 Variances in the Disposal Process

Departments are obligated to implement disposal authorities. Legitimate variances in the implementation of a disposal authority may occur. For example, disposal of records may need to be put on hold to accommodate ATIPP request, legal issues, etc. In the event that the regular course of business is interrupted resulting in an inability to dispose of information, the variance as well as the resumption of normal disposal operations should be documented.

4.0 Executing Disposal

4.1 Master Standing Offer Agreements

The Government Purchasing Agency maintains a number of Master Standing Offer Agreements that support the standard purchase of goods and services related to IM. This includes:

- Third Party Offsite Storage
- Secure Shredding Services
- Storage Boxes

Contact your financial operations officer to ensure that you are using the appropriate Master Standing Offer Agreement when procuring IM related services.

4.2 Secure Destruction

Whether a record is transitory or a government record that requires disposal authority, destruction should be done in such a manner that information contained within the record is made permanently inaccessible. This may be secure shredding in the case of paper records, or secure erasure or disposal of physical media in the case of electronic records.

4.2.1 Paper/Microforms

There are three options for the secure destruction of paper/microform records:

Option 1: Onsite Shredding by Departmental Employees.

- This option is best suited to the disposal of transitory records or in offices where the content is highly confidential and therefore warrants document level disposal (e.g., cabinet records).
- Onsite shredding is time consuming as the volume that can be processed varies depending on the size and quality of the shredder.
- It is important to ensure that the shredder output renders the records irrecoverable.
- If destroying government records, a record of the disposal authority, what was destroyed, by whom and when should be retained.

Option 2: Security Boxes onsite

- Security boxes are large shredding boxes with secure covers and locks. They are individually numbered by the vendor to allow for tracking and reporting.
- Security boxes are highly recommended for the disposal of transitory records as it is easy for employees to take materials to a centrally located security box.
- If used to destroy government records the department should keep a record of what is going into the box.
- A representative from the department should accompany the vendor to the loading area to witness the destruction of the records..
- A destruction certificate should be sent by the vendor to the department that indicates the contents of the box have been destroyed. This certificate should be retained by the department as per C-RIMS.

Option 3: Bulk Shredding

- In the event that there is a large volume of records to be destroyed a third party may be contracted to complete the process.
- Records are boxed by the department with records of their contents retained for reporting purposes.
- Boxes are taken by the vendor offsite for destruction.
- Vendor should return a destruction certificate to the department. The certificate should be retained by the department as per C-RIMS.

4.2.2 Electronic Records On the Shared/Network Drive

When records are deleted from the network drive by departmental employees, they are typically inaccessible to users of the shared or network drive. Departments are advised to ensure that appropriate documentation occurs in the event that government records are deleted from the shared or network drive. Back-up copies of this information are retained

by the OCIO as per the Backup Policy. After the prescribed period as per the Backup Policy has elapsed, any records deleted by departments are no longer accessible. Information related to the Backup Policy is available on the OCIO website.

4.2.3 Electronic Data

Electronic data retained within the business applications supported by the OCIO may constitute a government record. While the OCIO is the custodian of this data, the department is responsible for ensuring that the OCIO is provided with proper direction on the retention and disposal requirements related to data within a business application. Departments are responsible for developing RRDS to authorize the disposal of data maintained within business applications. The OCIO will work with the department to ensure that RRDS are implemented for this data and that reporting requirements related to disposal are met.

4.3 Transfer of Records to The Rooms Provincial Archives Division

The *Rooms Act* mandates the Provincial Archives Division to “*collect, preserve, present, exhibit and make available for research the historic artifacts, natural history specimens and archival records that represent and illustrate the significant history, culture and natural heritage of the province.*” TRPAD will determine whether records created by a department have enduring value and will work with the department to arrange the transfer of those records deemed to have such value.

Refer to TRPAD to ensure that appropriate procedures are followed to transfer custody of records.

5.0 Glossary

5.1 Definitions

[Disposal](#)

[Transitory Record](#)

5.2 Acronyms

ATIPPA	Access to Information and Protection of Privacy Act
OCIO	Office of Chief Information Officer
GRC	Government Records Committee
PRC	Provincial Records Centre
TRPAD	The Rooms Provincial Archives Division
RRDS	Records Retention and Disposal Schedule

6.0 References

[Management of Information Act](#)

[Information Management and Protection Policy, TBM 2009-335](#)

Government of Newfoundland and Labrador Corporate Records Information Management Standard 1 (C-RIMS) Manual

ISO.TR 15489-2: 2001 – Information and Documentation – Records Management – Par 2: Guidelines

Records Retention and Disposal Schedule (RRDS)

7.0 Revision History

Date Reviewed	Reviewed By
2010-12-17	Iris Power, Director of Information Management Services
2011-01-12	Shelley Smith, Executive Director Information Management
2011-01-14	Information Management Standards Board (IMSB)
2011-02-24	Government Records Committee (GRC)
2015-03-23	Bun Power, IM Consultant, IM Services



Government of Newfoundland and Labrador
 Office of the Chief Information Officer
 Information Management Branch

GUIDELINE – RECORD IMAGING SERVICES

Guideline (Definition): OCIO Guidelines derive from **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board as well as the **ATIPP Policy**. Guidelines are recommended actions, general approaches and operational behaviors. They recommend actions and are not compulsory, as they take into consideration the varying nature of information management programs. Guidelines are generally a description that clarifies what should be done and how to achieve the objectives set out in policies and directives (source: ISO/IEC 17799:2005).

Issuing Branch	Information Management Branch
Approval Date	
Review Date	2015 04 02
OCIO TRIM Number	DOC06443/2011
Authorizing Directive	Information Management and Protection Policy, TBM 2018-111 (replaces TBM 2009-335)
GRC Approval Date	2011 06 15
Related Directives	
Related Standards	Corporate Records and Information Management Standard (C-RIMS)
Related Guidelines	See References

APPROVAL AND SIGN OFF

Executive Director, Information Management Branch			
	(name)	(signature)	(date)

Note: Questions related to this guideline should be forwarded to im@gov.nl.ca

TABLE OF CONTENTS

- 1.0 Overview 1
- 2.0 Scope 1
- 3.0 Background 1
 - 3.1 Benefits 1
 - 3.2 How Imaging Works 2
 - 3.3 Types of Imaging Services 2
 - 3.4 Planning and Implementation Issues 3
 - 3.4.1 Record Value 3
 - 3.4.2 Software Requirements 4
 - 3.4.3 Storage 4
 - 3.4.4 Accessibility and Metadata 5
 - 3.4.5 Integrity, Reliability and Security 5
 - 3.4.6 Quality Control 6
 - 3.4.7 Centralized versus Decentralized 6
 - 3.4.8 Disposition 7
 - 3.4.9 Retention Format 7
 - 3.4.10 Employee Impact 8
 - 3.4.11 Outsourcing Imaging Services 8
- 4.0 4.0 Recommended Approach 9
 - 4.1 Identify the Business Need 9
 - 4.2 Document the Life Cycle 9
 - 4.3 Complete Records Inventory and Volume Assessment 10
 - 4.4 Define Scope and Flow of Service 10
 - 4.5 Update or Create a RRDS 10
 - 4.6 Technical Consultations 10
 - 4.7 Identify Physical Location Requirements 11
 - 4.8 Identify Roles and Responsibilities 11
 - 4.9 Estimate Resource Requirements 11
 - 4.10 Develop a Business Case/Requirements 11
 - 4.11 Obtain Approval for Imaging Service 12
 - 4.12 Procure Supplies and Services 12

4.13 Define Procedures..... 12

4.14 Provide Education and Awareness 12

5.0 Glossary..... 13

5.1 Definitions..... 13

5.2 Acronyms..... 13

6.0 References..... 14

7.0 Revision History 14

Appendix A: Imaged Record Format Options..... 15

Appendix B: Sample Image Quality Checklist 16

Appendix C: Information Life Cycle Questions..... 17

Appendix D: Imaging Services: Procedural Considerations 18

GUIDELINE – RECORD IMAGING SERVICES

1.0 Overview

Record imaging refers to the transformation of printed records into electronic format. An operator completes this process using a document scanner and imaging software. The purpose of the software is to capture metadata about the record including classification, security and descriptive information. This metadata allows the record to be securely stored and retrieved in the department's electronic repository. Many departments use imaging services to process, retain and make accessible records they receive in physical format. This guideline provides an approach to the development and operation of record scanning services.

2.0 Scope

This *Guideline* applies to or may be used by all public bodies, as defined in the *Management of Information Act*. Any references to department in this Guideline can be understood to include any public body. Its audience includes resources responsible for the operation of an Information Management (IM) program within a department.

3.0 Background

3.1 Benefits

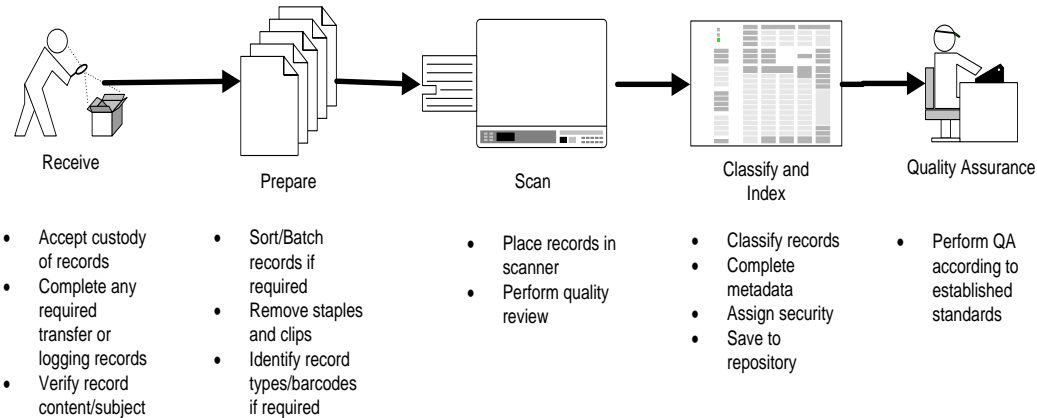
There are many reasons why a department may decide to develop imaging services.

- Real-time accessibility to records to support decision making
- Eliminate reliance on geographic proximity to records
- Consolidate physical and electronic records to enable users to access a complete file
- Automated application of retention and disposition authorities to improve compliance with legal and regulatory requirements
- Reduce need to retain copies of records thereby ensuring that the record of authority is managed properly
- Reduce the handling and use of fragile or heavily used original material and create a "back up" copy for endangered material such as brittle books or documents

3.2 How Imaging Works

Record imaging refers to the transformation of printed records into electronic format. Along the way, there are actions required to ensure that records are appropriately received, prepared, scanned, indexed and verified. Each of these phases must be carefully planned to ensure that the resulting imaged records are of high-quality, accessible to users and managed properly.

Figure 1: Sample Imaging Process



3.3 Types of Imaging Services

The way that departments deliver imaging services will differ depending on business need. The business need reflects why the decision is made to image records, what records need to be imaged and how users need to be able to use records. Some types of imaging services include:

- **On Demand:** Records are imaged at the request of employees or clients
- **Process Specific:** Records that support a specific process are imaged. Business processes are reengineered to ensure that records are imaged and classified to facilitate processing. This often includes use of workflow technology to route records automatically for review, action or approval
- **Image Retrieval:** Record imaging services are setup in a storage centre where records are imaged by operators for users on demand. Enables quick review online for users located outside easy transport distance
- **Mail Processing:** Imaging of mail classified as records when received by government. Requires reengineering of mail processing. Allows for capture of physical record on receipt
- **File Consolidation:** Use of scanning to consolidate files that consist of electronic and physical components. Case and client files are good candidates, as users need to have all information easily accessible. Often includes back-file conversion.

3.4 Planning and Implementation Issues

In developing imaging services there are a number of important issues to consider.

3.4.1 Record Value

Record value is an important factor when deciding what records to image. Resources required for imaging may be warranted for high-value records while the decision may be made to retain low-value records or records with specialized management requirements (e.g., archival) in physical format.

Figure 2: Identifying Records to Scan

Characteristics	Records to Image	Records to Retain in Physical Format
Record Use	<input type="checkbox"/> Essential to provision of service <input type="checkbox"/> Support transaction or client processing <input type="checkbox"/> Need to annotate files <input type="checkbox"/> Needed for collaboration <input type="checkbox"/> Need to action files via use of workflow <input type="checkbox"/> Multiple users at one time may require access	<input type="checkbox"/> Administrative files <input type="checkbox"/> Uncertain level of demand <input type="checkbox"/> Limited number of users <input type="checkbox"/> Used for reference only
Location of Users	<input type="checkbox"/> Users geographically dispersed <input type="checkbox"/> Users require immediate access	<input type="checkbox"/> Users located onsite <input type="checkbox"/> Access can be delayed for transport time
Office of Primary Responsibility (OPR)	<input type="checkbox"/> Department is OPR and is responsible for retention and disposal.	<input type="checkbox"/> Department is not OPR – copies are transitory
Rate of use	<input type="checkbox"/> Required to support critical operations	<input type="checkbox"/> Infrequent access (less than once every 3 months)
Length of retention	<input type="checkbox"/> Retention is required for a extensive time period	<input type="checkbox"/> Record with a short retention may not warrant cost of scanning
Retention format	<input type="checkbox"/> Records can be retained in electronic format provided quality scanning procedures are used	<input type="checkbox"/> Records must be retained in physical format
Conservation issues	<input type="checkbox"/> Records are compromised and cannot be handled in current condition <input type="checkbox"/> Scanning records will preserve fragile physical format	<input type="checkbox"/> Records are copies or can be easily reproduced
Disposition	<input type="checkbox"/> Records that have a final disposition of destroy	<input type="checkbox"/> Records that have a final disposition of Archive
Security and Access	<input type="checkbox"/> Sensitive information that will benefit from ability to control and track access to user network or system account	<input type="checkbox"/> Publicly accessible information requires no additional security measures

3.4.2 Software Requirements

Imaging services require both the scanner used to capture an image of the physical record as well as software that enables the record to be processed. Scanning software packages offer a range of benefits to accommodate business needs. Some functionality available via the software includes:

- Batch processing – ability to process multiple individual records
- Barcode Integration – ability to read/apply barcode data to records
- Optical Character Recognition (OCR) – Ability to extrapolate data from imaged records and apply it as metadata
- Intelligent Character Recognition - Ability to extrapolate handwritten data from imaged records and apply it as metadata
- Image upgrade – Ability to upgrade image quality (e.g. De-speckle, de-skew, adjust brightness and contrast)
- Annotation tools – Ability to add notes to records (e.g. electronic post-it)
- Workflow Integration – Ability to define and automate a business process that will route the imaged record to user for approval or action
- Integration with business or process specific applications including case or client management to consolidate information in one format or text redaction software used for ATIPP request processing.

The types of features users need will vary depending on business need and intended use. If records are standard letter-size documents used only for reference then fewer software features are needed that if records are varying sizes, sources and quality that must be acted on. Understanding the business need is critical to ensuring the right software is chosen and properly configured. Consulting with the OCIO to map requirements to software functionality is critical when considering developing imaging services.

3.4.3 Storage

How and where records are stored has an impact on the overall imaging service. Imaged records can be stored in various locations including shared drives, Electronic Records Management Software (ERMS) like TRIM or in offline storage. Deciding where records are most efficiently stored must consider many issues. This includes existing practices in the department (e.g., TRIM is already in use and can be expanded), process requirements (e.g., ability to use workflow is a requirement) and security considerations (e.g. access must be limited and tracked).

Imaged records typically require a larger amount of storage space than word-processing documents depending on the file format used. Additional information on imaged file format options is included in Appendix A *Imaged Record Format Options*. It is important to ensure that the storage space required is estimated properly and can be accommodated. Consult with OCIO to discuss storage requirements prior to developing imaging services.

3.4.4 Accessibility and Metadata

Electronic records are accessed and used at the record level as opposed to being grouped together in a paper file folder. This means that electronic records need to be organized in a way that ensures accessibility. Electronic records benefit from the use of metadata, or information about the record, that can be used to retrieve and manage it. Elements like the file name, classification, type of record, relation to other records, access and security, author, etc. are examples of record metadata. The best time to add metadata about a record is at the point when it is imaged. Some software applications automatically populate some metadata or allow for predefined lists or lookup tables that make it easier to consistently capture metadata. Considerations related to metadata include:

- Knowing how users will need to access and use the information is important to consider when establishing metadata
- Retention, disposal and security requirements are also needed to determine metadata
- Be reasonable in what you expect operators to apply to every record. While it may be possible to record extensive information about each image, is it necessary? Will the metadata actually be used to manage or retrieve information?
- Understand what metadata can be automatically populated based on set properties, a barcode or even data from another business application
- Ensuring that operators have a clear understanding of how to apply metadata is important in ensuring that it is consistently applied to all records.

3.4.5 Integrity, Reliability and Security

Integrity means safeguarding record accuracy and completeness. From an imaging perspective, this means that the scanned copy must be an accurate reflection of the original and that it has not been modified during the imaging process or subsequent use. Implementing quality control in the imaging process is important to support record integrity. Records management policies and procedures should specify what additions or annotations may be made to the record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable. A benefit of imaging is that software can be used to annotate records and actions are traceable through an audit trail.

A reliable record is one whose contents can be trusted as a full and accurate representation and can be depended on. From an imaging perspective it is important to ensure that the role of imaging in the business process is clearly understood. With the enhanced tracking features applied against the records by the software, the ability to track record receipt and use can be used to support reliability.

Security as it relates to records combines the properties of authenticity, reliability with access control. The issue of whether the electronic format of records may present risks to integrity, reliability and security is often debated. While being in electronic format allows for easier distribution (e.g. via e-mail), when records are imaged properly as a part of an audited program defined processes combined with the software features should make it possible to apply appropriate security and track use.

3.4.6 Quality Control

A successful imaging service relies on high-quality images. Quality is important for many reasons including:

- Users need to have clear and reliable content on which to base business actions and decisions
- If the quality of the imaging service is questioned, decreased confidence in the image to act as authentic and reliable records will impact management and use
- Poor quality images compromise the ability of records to act as electronic evidence of the government's business activities.

Software features that may be used to support business processes may not work properly if image quality is poor. For example, the ability of software to use OCR to read text in images

- Staff must be properly trained to perform scanning and related activities to ensure that they understand how to process, scan and handle records
- Equipment must be appropriate for the records to be imaged (e.g. the size and quality of the scanner must be appropriate for the record format (e.g. oversized records must have an appropriate scanner, if the need is to scan many records at one time then a scanner with a batch processing capability is required, etc.)
- Equipment must be checked to ensure it is operating properly, is clean, etc.
- Images must be accurate and reliable copies of the original. Appendix B *Sample Image Quality Checklist* provides an example of the features to check to verify image quality.

Periodic audit and review of image quality (e.g. random samples) as well as the imaging process are recommended to ensure ongoing quality of the imaging service.

3.4.7 Centralized versus Decentralized

Determining whether there is a need to centralize or decentralize scanning services has an impact on resources and staffing.

Centralized scanning limits the number of scanning locations. This allows for dedicated operators to complete scanning and associated activities including classification and indexing. Scanning is typically centralized when anticipated volumes are high or there is a need for extensive back file conversion. A benefit to this approach is that operators develop and maintain expertise in scanning processes. Also, the larger volume of records justifies larger, better quality scanning hardware. More sophisticated machines are able to reliably process larger batches of records thereby reducing processing time.

Decentralized scanning is effective to process specific records that tend to be lower volume (e.g., executive correspondence management). This is because the operators are typically not dedicated to scanning records. The requirement to scan overlaps with other duties (e.g. administrative assistant). When planning to implement decentralized scanning as a part of a process it is important that IM is incorporated into the planning, implementation and review process to ensure that operators are properly trained and supported to ensure quality images.

Many work areas are now equipped with a multi-function printer that allows employees to scan and e-mail records. This feature can be disabled if required. It is important to consider

how and if this feature will be used as a part of the overall IM program within the department. Refer to the OCIO Guideline *Information Management (IM) Policy Instruments* for guidance on developing a departmental policy, standards or guideline on this function. When instruction to employees is available, refer to the OCIO Guideline *Information Management (IM) Education and Awareness for Government Employees* to develop a plan to train and support employees.

3.4.8 Disposition

A records retention and disposal schedule (RRDS) is a legal document that guides the management of a government record. A RRDS will:

- Define the content of the record series or types
- Link the records to the organizational unit and business process
- Dictate how long the records need to be retained in active and semi-active storage to meet operational and legislative requirements
- Authorizing the disposal of information in a legal manner including either secure destruction or transfer to The Rooms Provincial Archives Division (TRPAD).

Understanding disposal requirements is critical in planning imaging services as it is a determining factor in information handling, retention and disposal. Points to consider include:

- All records must be disposed of in a secure and timely manner
- The quality of imaged records must be verified prior to disposal actions
- Transitory and non-OPR records should be securely destroyed as soon as no longer required for reference purposes.
- If imaged records are non-OPR records then verify with the OPR how long records are retained to ensure that the department does not exceed the legal retention requirement
- Imaged records that are transitory or that belong to another OPR are still discoverable and must be processed by the department in possession of them in the event of litigation, ATIPP requests, etc.
- Ensuring that there is an updated RRDS for records to be imaged is the first step to ensuing efficient disposition.

3.4.9 Retention Format

The RRDS includes descriptive information about a group of records. It is recommended that the RRDS include references to the format that records are retained in. This includes whether records are imaged, how they are stored, etc. The *Management of Information Act* permits the use of an electronic record as a government record. Section 4.1 requires that:

a) the electronic information is retained in the format in which it was made, sent or received or in a format that does not materially change the electronic information that was originally created, sent or received; and

(b) the electronic information will be accessible, and capable of being retained for subsequent reference, if required, by a person who is entitled to have access to the information or who is authorized to require its production.

Physical records that are imaged following industry and government standards for quality can be recognized as a transitory record and securely destroyed provided there are no legal or management requirements that preclude this action. For example, records that must be retained in physical format or those with a disposition of Archive must be retained. OCIO strongly cautions that maintaining both imaged and paper versions of the same records creates added cost and burden both for departmental staff and IT systems, and should be avoided.

3.4.10 Employee Impact

When planning imaging services it is important to consider the impact that introducing the imaging component to the business process will have on employees. This includes IM employees as well as departmental employees involved in the processes in which imaging is introduced.

For IM staff, record imaging may require education and awareness on scanning and business processes. This may include:

- Knowledge of cataloging, registration methods, or metadata
- Familiarity with conservation methods
- Understanding of scanning techniques and methods
- Computer skills and imaging certification

If existing employees do not possess the appropriate skills to perform imaging service requirements training and support is required. Note that depending on how the service will be delivered, imaging operators may not necessarily be IM staff (e.g. the TRIM Executive Correspondence process requires administrative staff to scan incoming correspondence). Employees who are accustomed to accessing their records in paper format will need to understand how imaging impacts their existing process. They will require guidance on how to engage services, how to access, modify or annotate records and where to go for support when required. Education, ongoing awareness and support will ensure that the introduction and use of imaging is successful.

3.4.11 Outsourcing Imaging Services

When the scope of the service, nature of the records and resource requirements are considered, a decision may be made that imaging services will be available to the department but will be completed by a third party. Outsourcing is often used when:

- There is a large volume to scan or a backlog of records to transform
- Records are imaged at the end of the process as opposed to somewhere in the middle

- Records do not require workflow (e.g. they don't need to be scanned as soon as they arrive at the department and then routed)
- Record processing can be delayed (e.g. records are not so critical that the delay to transport and process by a third party is unacceptable)
- Staffing or technical resources are not available with the department

The following table lists some of the pros and cons of outsourcing:

Outsourcing Pros	Outsourcing Cons
Pay for cost of scanning documents only, not equipment or staffing	Complex contractual process: specifications must be clearly defined up front
Vendor has the equipment in place to process high volumes of records quickly	Originals must be transported, shipped, and then also handled by vendor staff
On-site expertise as opposed to having to provide ongoing education and awareness for staff	Departmental staff lose the opportunity to develop imaging skills
Transfer risk of quality issues to the vendor	Department has less control over process, quality control
Vendor absorbs costs of technology obsolescence, failure, downtime, etc.	
Faster time to service as minimal assessment, configuration and implementation time is required	

4.0 4.0 Recommended Approach

4.1 Identify the Business Need

Determining the business need is the first step in developing an imaging program. Defining why records are to be imaged, how records will be used and what the management requirements impact how the services is established and operated. When determining business need:

4.2 Document the Life Cycle

The life cycle refers to the stages through which information is managed. It is important to manage records in a manner that supports authenticity, reliability, integrity and usability throughout all stages including:

- Creation and organization;
- Receipt and capture of data;
- Retrieval, processing, dissemination and distribution of data;

- Storage, maintenance and protection;
- Disposal, including secure destruction or transfer to The Rooms Provincial Archives Division

Documenting the typical life cycle of the records that will be imaged will be helpful in finalizing requirements and developing operational procedures. Appendix C, *Information Life Cycle Review* includes typical questions to consider when documenting the life cycle.

4.3 Complete Records Inventory and Volume Assessment

Use the OCIO guideline *Records and Information Inventory* to get an understanding of the records and their volume. Note during the inventory any special considerations that will impact the imaging process including:

- Special format or irregular sizes
- Conservation issues
- Existing organization (e.g. are records already organized or will processing need to be performed to batch records for scanning)
- What is the backlog volume (if any) to be imaged?
- What is the estimated daily, weekly, monthly and/or annual volume?
- What will happen to records following scanning?

4.4 Define Scope and Flow of Service

Based on the business need, life cycle of records and the volume of records, define the services that are required to support imaging. Note the impact to employees for consideration in training and implementation. For example, if records are imaged at the end of a business process there may be minimal impact on employees. If a business process is modified to incorporate the imaging of records early in the process (e.g., executive correspondence managing using TRIM) then there will be an impact on the scope and cost of implementation as additional training and support resources may be required

4.5 Update or Create a RRDS

Update or create a RRDS for the records that will be imaged. This will ensure that all management requirements are documented and approved by all stakeholders including TRPAD.

4.6 Technical Consultations

In planning imaging services it is essential to consult with IT experts on the options available and service requirements to establish and maintain the imaging service. Contact the Planning and Service Delivery Committee (PSDC) chair to consult with OCIO on technical requirements.

4.7 Identify Physical Location Requirements

Understand where the imaging process will occur. Refer to the OCIO guideline *Physical Records Storage Development and Use* for information on space allocation and planning. The need to perform centralized versus decentralized scanning greatly impacts this assessment. At a minimum the location will require:

- Space for employees to receive and log records
- Staging area to prepare records for digitization
- Space allocated for scanner equipment
- Computer workstation(s)
- Space allocated to prepare records for disposal (e.g. secure shredding, transfer to TRPAD)

4.8 Identify Roles and Responsibilities

Based on the services that are required, determine the roles and responsibilities required to support the imaging service. Refer to the information related to this area of program development in the OCIO guideline *Information Management (IM) Governance, Accountability and Organization*. Map roles and responsibilities to existing employees or identify the need to have new resources allocated to support the imaging process.

4.9 Estimate Resource Requirements

Estimate the resources required to establish and operate the imaging service. This may include:

- Procurement of hardware/software
- Scanner and software configuration
- Physical space modifications to accommodate services
- Employee salary and support costs

4.10 Develop a Business Case/Requirements

If you are implementing a new scanning service of function, it may be necessary to develop a business case. Based on your assessment prepare a description of the physical storage required, services that will be provided and all associated costs. Components may include:

- Business need: based upon an inventory and assessment of the types and volume of records needed in active storage
- Services to be provided: filing, faxing, mail pick-up processing and delivery, secure disposal, etc.
- Scope of the records to be stored: all active records, records of only certain program areas, all media types, etc.
- Staffing impact/requirements: staffing of the function or management of the function through periodic visits for record retrieval or disposal and spot checks as required

- Total set-up cost: include cost of equipment, facility augmentation, software, services, etc.
- Total operating costs per year: include supplies, licensing or leasing costs, maintenance costs for equipment such as scanners, etc.
- Return on Investment: savings to be accrued by freeing up office space to be used for staff or by cutting costs for commercial storage
- Intangible benefits: highlight benefits to the processes impacted by imaging including faster access to information, consolidated files, ability to track access and use, quicker response times, etc.

4.11 Obtain Approval for Imaging Service

Requirements will vary depending on many variables including the existing space allocated (if any), required physical upgrades, and addition of new or modification of existing support services. Ensure approval of the Executive for implementation expenses and ongoing operations. Verify whether other stakeholders need to be engaged including OCIO, Transportation and Works, departmental financial operations and human resources.

4.12 Procure Supplies and Services

Working with departmental stakeholders and Transportation and Works, identify and procure the supplies and services required to complete any upgrades or modifications to the location in which imaging will occur. Refer to the OCIO guideline *Physical Records Storage Development and Use* for information on location planning. All scanners, computers, software, etc. related to imaging must be procured through the OCIO. Contact information and Forms are available on the OCIO website. For new or significantly modified services, it is advised to consult the OCIO via your departmental PSDC chair.

4.13 Define Procedures

Establishing consistent procedures is essential in ensuring that records are managed as per legal, regulatory and operations requirement and that services are consistent.

- Services
- Operations
- Security

Considerations for the planning and development of procedures have been included in Appendix D, *Imaging Services: Procedural Considerations*.

4.14 Provide Education and Awareness

Based on the services provided, staff may require training on imaging concepts, use of equipment and software. Also, frontline staff will need to understand the imaging process as it relates to business activities. Refer to the OCIO Guideline *Education and Awareness for Information Management Practitioners* for information for on support required for IM staff.

Prior to the start of operations and at appropriate intervals thereafter, communicate to departmental staff:

- Services offered
- How to access services including after hours (if applicable)
- Hours of operation for scanning
- Contact Information

Use the OCIO Guideline *Education and Awareness for Government Employees* to develop a communications strategy. Things to consider:

- Create a unique e-mail and phone number for the service (if centralized)
- Ensure that staff know how to initiate service
- Ensure that information is readily available (e.g. Departmental Intranet if one is available)
- Consider marketing materials (e.g. posters, handouts, etc).

5.0 Glossary

5.1 Definitions

[Electronic Records Management Software](#)

[Information Management](#)

[Integrity](#)

[Office of Primary Responsibility](#)

[Records Retention and Disposal Schedules \(RRDS\)](#)

[Reliability](#)

[TRIM](#)

5.2 Acronyms

ERMS	Electronic Records Management Software
IM	Information Management
IT	Information Technology
PSDC	Planning and Service Delivery Committee
TRPAD	The Rooms Provincial Archive Division
OCR	Optical Character Recognition
OPR	Office of Primary Responsibility

6.0 References

Management of Information Act

Information Management and Protection Policy, TBM 2009-335

Guideline – Education and Awareness for Information Management Practitioners

Guideline – Information Management Education and Awareness for Government Employees

Guideline – Information Management Governance, Accountability and Organization

Guideline – Physical Records Storage Development and Use

Guideline – Records and Information Inventory

7.0 Revision History

Date Reviewed	Reviewed By
2011-05-27	Iris Power, Director, Information Management Services
2011-05-30	Shelley Smith, Executive Director, Information Management
2011-06-06	Information Management Standards Board (IMSB)
2011-06-13	Government Records Committee (GRC)
2015-04-02	Bun Power, IM Consultant, IM Services

Appendix A: Imaged Record Format Options



File Format Options
for Imaged Records 2

Appendix B: Sample Image Quality Checklist



Image Quality
Checklist 20110526.d

Appendix C: Information Life Cycle Questions



Information Life
Cycle Questions v1.21

Appendix D: Imaging Services: Procedural Considerations



Imaging Procedural
Considerations 2011C