Document Title:

Information Management and Protection Policy

Document Type: Policy	**No. Of Pages** (11)

Scope: Government of Newfoundland and Labrador and Public Bodies supported by the Office of the Chief Information Officer (OCIO)

Trim (#) DOC18385/2009	**Revision (#)** 2	**Treasury Board Approval (#)** TBM 2009-335

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*.

Date Created	Review Date	Lead Branch	Corporate Operations and Client Services	Treasury Board Approval
2009-11-19	2013-01-04 Every 2 years from the above date	Information Management	Shelley Smith Executive Director (A)	TBM 2009-335

Table of Contents

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* 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 willfully breaching confidentiality of personal information may be subject to penalty under Section 72 of the *Access to Information and Protection of Privacy 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 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:

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 Provincial Archives 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 Provincial Archives.

8.0 Roles and Responsibilities

Groups	Responsibilities
OCIO	• 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	• Approve and/or recommend policies, directives, standards, guidelines and procedures for information protection and security. • Address 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 OCIO Senior Leadership Team (SLT).
Government of Newfoundland and Labrador Departments and Public Bodies ("Government")	• 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 *Management of Information Act, 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	• Comply with the *Management of Information Act* and the *Access to Information and Protection of Privacy Act.* • Comply with the Information Management and Protection Policy.
Cabinet Secretariat	• Responsible for policy direction for Cabinet Records in accordance with Section 5.4(1) of the *Management of Information Act.*
Treasury Board	• Approves Government of Newfoundland and Labrador policies.
Government Records Committee	• 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) Director's Forum	• 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	• Advises and educates public bodies on the appropriate and consistent application of the *ATIPP Act.* • 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	• 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 every two years and will be 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 (Source: *Management of Information Act SNL2005 c.M-1.01*).

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* 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 Provincial Archives;

- 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 (Source: *Management of Information Act SNL2005 c.M-1.01)*.

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 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 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 SNL2005 c.M-1.01.*

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). It is chaired by the Director of Information Protection, IM Branch.

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 (Source: *Access to Information and Protection of Privacy Act SNL2002 CHAPTER A-1.1).*

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 (Source: *Management of Information Act SNL2005 c.M-1.01*).

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*).