Guideline

Information Protection

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 Planning and Transformation Information Management Services
Original Issue Date:	2011-04-14
Date Last Reviewed:	2023-10-26
OCIO Reference:	DOC04993/2011
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 Information Protection Principles 9

5.0 Recommended Approach 10

5.1 Understanding Information Protection Capacity 10

5.2 Review Legislative and Policy Framework 11

5.3 Develop a Records Inventory 11

5.4 Physical, Technical, and Administrative Safeguards 12

5.5 Education and Awareness 12

6.0 Roles and Responsibilities 13

7.0 Supporting Materials and Version History 14

1.0 Overview

Protection is a major component of Information Management (IM). Information Protection (IP) typically focuses on inappropriate access or use of information.

IP represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, departments and other public bodies are required to protect information as part of their accountability under Section 6 of the Management of Information Act (MOIA).

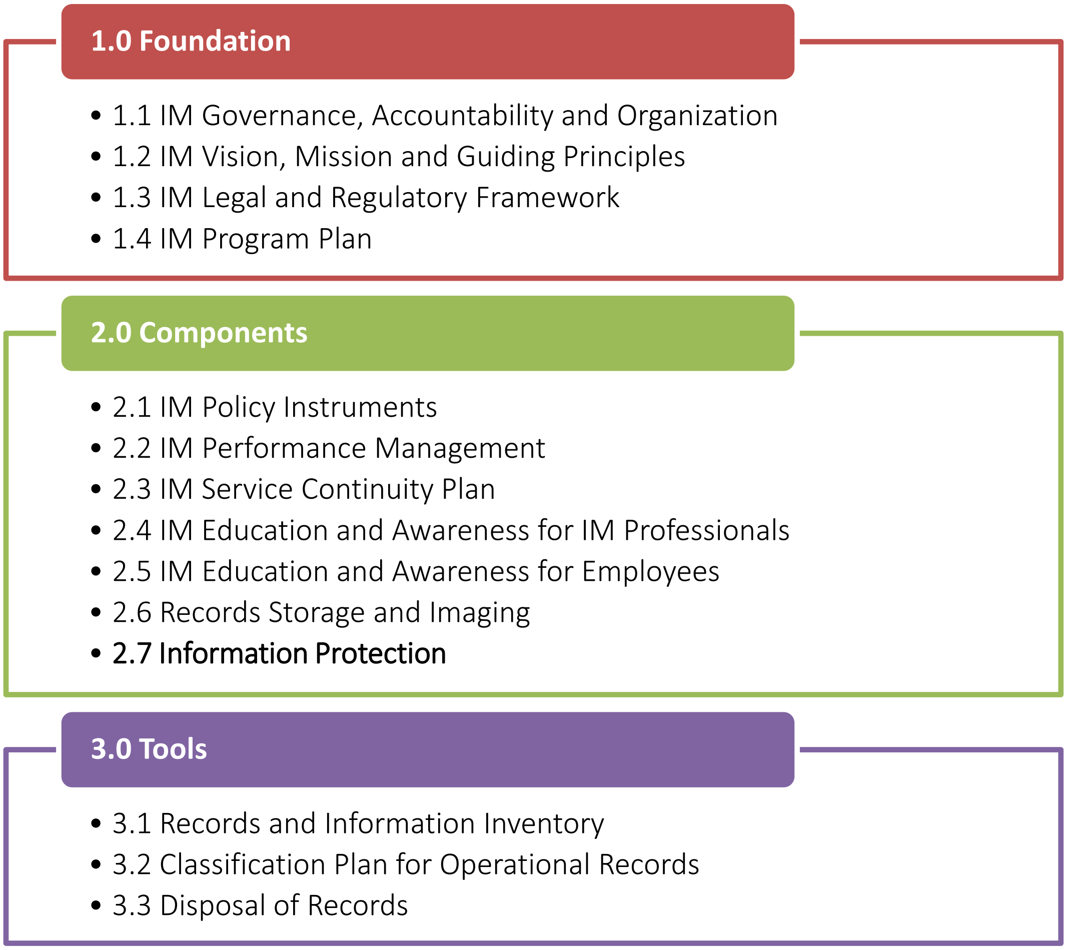
This Information Protection Guideline provides IP guidance and best practices that should be incorporated into a department or public body's overall IM Program. Guidelines are recommended actions, general approaches and operational behaviors. Generally, guidelines are a description that clarifies what should be done and how to achieve the objectives set out in policies, directives and standards.

Guidelines issued by OCIO provide a recommended approach, as they take into consideration the varying nature of information management programs.

2.0 Purpose

The Guideline – Information Protection 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 the MOIA for permanent heads of departments and other public bodies to implement a records and information management system.

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 Management
- 2.3 IM Service Continuity Plan
- 2.4 IM Education and Awareness for IM Professionals
- 2.5 IM Education and Awareness for Employees
- 2.6 Records Storage and Imaging
- 2.7 Information Protection

3.0 Tools

- 3.1 Records and Information Inventory
- 3.2 Classification Plan for Operational Records
- 3.3 Disposal of Records

Graphic: 1 - GuideBook Contents

Expected Deliverable(s)

1. The development and implementation of processes to support the organization's protection of government information.

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.

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).

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: ITIL).

Confidentiality – Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (Source: ISO 13335-1:2004).

Individual – For the purposes of OCIO IM policy instruments the definition of individual refers to all staff/employees, 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 departments and other public bodies as defined under the MOIA.

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 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.

Integrity – Integrity is the property of safeguarding the accuracy and completeness of assets. Integrity demonstrates that the record is complete and has been unaltered. It is necessary that a record be protected against unauthorized alteration. 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 (Source: ISO 15489:2001 and ISO 13335-1:2004).

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, 2015).

The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
ATIPPA	Access to Information and Protection of Privacy Act, 2015
IM	Information Management
IM&P	Information Management and Protection
IMCAT	Information Management Capacity Tool
IP	Information Protection
MOIA	Management of Information Act
OCIO	Office of the Chief Information Officer
PHIA	Personal Health Information Act

4.0 Information Protection Principles

IP promotes the protection of Government information by understanding information sensitivity and placing reasonable safeguards around information relative to its sensitivity; the more sensitive and/or personal the information, the more safeguards should be put in place to protect that information.

Information sensitivity can be determined by evaluating the information's value to an organization based on its Confidentiality, Integrity, and Availability requirements.

- Confidentiality – The practice of upholding required legal restrictions against unauthorized access or disclosure of information. This would include personal information, as defined in the Access to Information and Protection of Privacy Act (ATIPPA) and personal health information, as defined in the Personal Health Information Act (PHIA).

- Integrity – The practice of safeguarding the accuracy and completeness of information; maintaining the authenticity and preventing unauthorized modification or destruction of information.

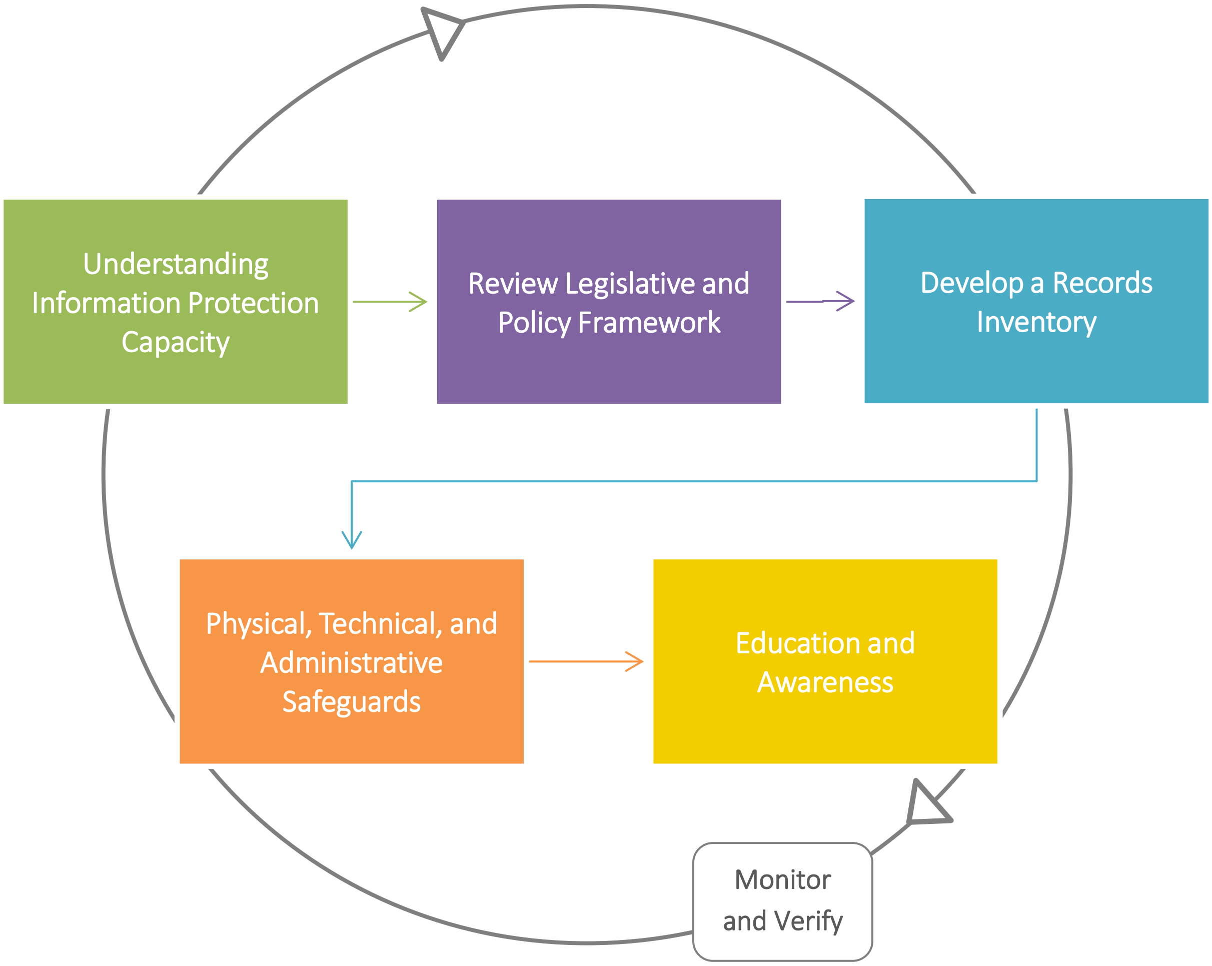
- Availability – The practice of making information accessible and useable upon demand by an authorized user; ensuring timely and reliable access to and use of information.

Information collected and maintained by the Government of Newfoundland and Labrador must be securely managed. To effectively protect information, it is important to understand the types of sensitive information maintained by a department or public body and the level of risk if those records were inappropriately disclosed.

5.0 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, implementation, and management of an effective IM Program through the protection of sensitive and personal information.

The following guidance will help departments and public bodies assess their current capacity to implement IP best practices and improve IP capabilities within their IM Program.



Understanding Information Protection Capacity
Review Legislative and Policy Framework
Develop a Records Inventory
Physical, Technical, and Administrative Safeguards
Education and Awareness
Monitor and Verify

5.1 Understanding Information Protection Capacity

To understand where a department or public body's processes rank from an IP perspective, it may be useful to complete a review of what the current practices are to protect personal and sensitive information in daily business transactions.

If the department has completed an Information Management Capacity Assessment, using the IM Capacity Assessment Tool (IMCAT), much of the information required in assessing the state of IP in your organization may already be captured and recommendations may already exist.

The following areas should be considered by departments and public bodies when assessing IP capacity:

- Review Legislative and Policy Framework
- Develop a Records Inventory
- Physical, Technical, and Administrative Safeguards
- Education and Awareness

5.2 Review Legislative and Policy Framework

Requirements around protecting information are often driven by legislation and policies. To understand what IP best practices should be developed to support an IM Program, a department and public body should have a good grasp of all legislation and polices that impact the organization from an information protection perspective. This includes provincial and federal legislation and well as Government-wide and organizational-specific policies. If a Legal and Regulatory Framework has been completed for your department or public body, this document will be vital to understanding necessary compliance requirements. The OCIO Guideline – Legal and Regulatory Framework outlines how to complete a comprehensive list of the IM compliance requirements that a department or other public body must satisfy.

5.3 Develop a Records Inventory

A records and information inventory is an important tool to support the implementation of IP activities within an IM Program. An inventory will enable employees to identify the volume and location of sensitive information that should be protected. 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.

5.4 Physical, Technical, and Administrative Safeguards

When protecting information, safeguards should be put in place relative to the sensitivity and criticality of the information they are meant to protect. Within departments and public bodies, safeguards can be physical, technical, or administrative in nature.
Physical safeguards monitor and control the physical work environment (e.g., locks on doors and cabinets, card access systems, video surveillance, security guards, etc.).

Technical safeguards monitor and control access to electronic information and computer systems (e.g., usernames and passwords, auditing, and encryption, etc.). It is important to note that most technical safeguards are maintained by IT professionals in an organization.

Administrative safeguards provide a framework for operating and managing the work environment (e.g., policies, privacy training, and security clearances, etc.).

5.5 Education and Awareness

Availing of existing information available through various stakeholders is a good way to kick-start an IP program. Use the IM Education and Awareness Guidelines to develop departmental plans around IP education and awareness. In addition, the ATIPP Office maintains an educational program for departments and public bodies subject to ATIPPA. Contact your organization ATIPP Coordinator for more information.

6.0 Roles and Responsibilities

Deputy Minister or Permanent Head or Designate (Department or other Public Body)

- Support the department or other public body's compliance with MOIA as well as OCIO-issued policies, directives, standards and guidelines, and ensure that proper protocols are in place to properly develop and manage a records and information management system, often referred to as an IM Program.

Directors responsible for IM

- Align organization-issued materials with the guidance provided by the OCIO in the development and implementation of a records and information management system, often referred to as an IM Program.
- Apply a continual improvement approach to the management of the organization's IM Program.

Office of the Chief Information Officer

As part of OCIO's administration of the Management of Information Act, the OCIO:

- Recommends to Treasury Board policies for adoption.
- Develops, manages, monitors, and communicates IM&P policy instruments and supporting materials to departments and other public bodies.
- Provides direction on IM&P best practices, resource requirements, organizational structure, recordkeeping systems and IM Programs to departments and other public bodies.
- Assists departments and other public bodies to improve their IM&P capacity.
- Provides IM&P advisory, training and awareness services and support to departments and other public bodies.
- Supports IM forums, committees, and other professional practice communities, consisting of IM representatives from departments and other public bodies.
- Manages the Provincial Records Centre (PRC).
- Provides administrative support to the Government Records Committee (GRC).

In addition, the OCIO will:

- Develop, implement, and maintain this Guideline as well as the GuideBook, also known as the Guide to IM for Public Bodies.
- Provide education and awareness on the implementation of an IM Program Plan.

7.0 Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published location.

Management of Information Act
http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Information Management and Protection Policy
https://www.gov.nl.ca/exec/ocio/files/policy-information-management-and-protection.pdf

Access to Information and Protection of Privacy Act, 2015
http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm

OCIO Website
https://www.gov.nl.ca/exec/ocio/

Information Management and Protection (IM&P) Glossary of Terms
https://www.gov.nl.ca/exec/ocio/im/glossary/

Personal Health Information Act
https://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2011-04-14	Version 1
2015-04-01	Version 2
2023-10-26	Version 3