Office of the Chief Information Officer

Managing Government Information Policy	
Office of the Chief Information Officer **Province of British Columbia**	**Version 1.0** **Date: June 19, 2020**

TABLE OF CONTENTS

INTRODUCTION

Purpose

This policy sets out ministry obligations for managing government information, specifically as they relate to *Information Management Act* (IMA) requirements.

Overview

The Province of British Columbia is the steward of a significant amount of government information, including data and records. This policy is meant to help ministries understand their high-level information management (IM) obligations and must be considered in conjunction with:

- applicable legislation, including but not limited to the IMA and the *Freedom of Information and Protection of Privacy Act* (FOIPPA);
- the Core Policy and Procedures Manual, specifically Chapter 12: Information Management and Information Technology Management;
- directives and guidelines issued by the Chief Records Officer (CRO) under the IMA; and
- corporate policies, standards and strategic direction issued by government, including the Standards of Conduct for BC Public Service Employees, the Draft Principles that Guide the Province's Relationship with Indigenous Peoples, the Province's Digital Principles, and policies and standards issued by Office of the Chief Information Officer (OCIO).

The OCIO, which is led by the Government Chief Information Officer (GCIO) and includes the CRO, is the central authority responsible for government IM and information technology (IT). Both the GCIO and the CRO collaborate with ministries to set corporate policies, standards and guidelines related to IM. The OCIO's Government Records Service (GRS) supports the CRO in providing expert advice and services to help ministries meet their IM obligations.

Ministries are encouraged to follow best practices in choosing IM approaches to help them achieve their mandates and support their ability to comply with applicable legislation and policy. Ministries should consider both the business value to their ministry as well as the corporate value of the information in their custody or control.

The Province of British Columbia is committed to reconciliation, equity and developing an efficient public service that is representative of the diversity of the people of British Columbia. To support a government where the needs of all people are reflected, ministries should consider opportunities to address these commitments throughout the information lifecycle.

Application

This policy applies to all ministries subject to the Core Policy and Procedures Manual.

Authority

Core Policy and Procedures Manual Chapter 12.

Advice on this Policy

For questions or comments regarding this policy, please contact:

Strategic Policy and Legislation Branch
Office of the Chief Information Officer, Ministry of Citizens' Services
Email: IM.ITpolicy@gov.bc.ca

For questions or comments regarding corporate information management services, please contact:

Government Records Service, Corporate Information and Records Management Office
Office of the Chief Information Officer, Ministry of Citizens' Services
Email: GRS@gov.bc.ca

POLICY REQUIREMENTS

Government information is a strategic enterprise asset that must be managed in accordance with its value. Efficient and effective IM:

- supports the design, development, implementation and evaluation of government programs, services, policies, standards, processes and procedures;
- fosters informed decision making and effective risk management;
- facilitates accountability, confidentiality, transparency and collaboration, and allows government to be more responsive to British Columbians;
- maintains evidence of and information about business activities, transactions and decisions;
- ensures government information is preserved for as long as it is required, and is appropriately transferred to the government archives if it is determined to have permanent value; and
- ensures accessibility, discoverability and usability of information over time.

1. Creation and Use

Ministries should apply the principles, standards and practices of the records management discipline to managing government information in their custody or control. This includes information ministries create and receive. Taking a lifecycle approach to understanding and managing government information will help ministries meet their IM obligations.

Managing and Protecting Information

1.1 Ministries must be aware of, and able to account for, the information in their custody or control. This includes identifying, capturing, documenting and managing government information in accordance with applicable legislation, policies, standards and procedures.

1.2 Ministries must protect the integrity, authenticity and reliability of government information in their custody or control.

1.3 Ministries must ensure that information is adequately identifiable so it can be managed throughout its lifecycle. This includes:

a. applying appropriate and consistent metadata to information in accordance with applicable metadata standards and other relevant requirements;
b. using naming conventions; and
c. applying information schedules.

1.4 In cases where government information is duplicated for the same purpose by more than one office, or is created collaboratively, an office of primary responsibility (OPR) must be clearly

identified. The OPR must manage the information, including substantive drafts, according to the appropriate information schedule.

Access

1.5 Ministries must make information in their custody or control accessible and discoverable as appropriate. To this end, records should be legible/readable, available, and searchable for employees who need to access the records.

1.6 Ministries must be able to locate information in their custody or control in a timely manner.

Critical Information

1.7 Ministries must identify critical information in their custody or control.

1.8 Ministries must ensure that critical information in their custody or control is protected in a manner that will allow the information to retain its integrity and remain reliable, usable, accessible, and secure for as long as needed.

Appropriate Systems

Section 19 (1) of the IMA requires ministries to have an appropriate system in place for managing and securing government information. There are also various corporate policies and standards that contain requirements associated with managing and securing government information in an appropriate system, including but not limited to the following:

- Information Security Policy
- Privacy Management and Accountability Policy
- Digitizing Government Information Standard

The IMA also requires that ministries have an appropriate system in place for creating and maintaining government information that is an adequate record of their decisions. The CRO Directive on Documenting Government Decisions sets out the components of an appropriate system for creating and maintaining government information that is an adequate record of decisions.

The policy requirements below are meant to help ministries meet their obligations as per section 19 (1) of the IMA.

1.9 When establishing a system for managing records throughout their lifecycle, ministries must ensure they meet the requirements of an appropriate system.

1.10 Ministries must ensure that government information and data are stored in systems and facilities that are monitored and maintained with appropriate privacy, security, access and environmental controls.

1.11 Ministries must design, implement and maintain IM and IT systems with due consideration for information retention, destruction, privacy and access requirements.

1.12 Each ministry must maintain an inventory of all the systems it uses to manage information in its custody or control.

1.13 Ministries must ensure they can, for each of their IM systems, identify and measure:
   a. the range of risks;
   b. vulnerability to threats;
   c. ministry roles and functions in crises; and
   d. potential business impacts in the event of system issues.

2. Classification, Scheduling and Appraisal

As outlined in sections 10 and 11 of the IMA, government information must be managed in accordance with applicable information schedules. This ensures that government records:

- are linked to their business context through classifications;
- are retained as required according to authorized timetables; and
- are transferred to the government archives, destroyed according to authorized timetables, or approved for removal to a non-government organization. For guidance, see RIMM 504 Records Transfer Outside of Government.

Within the Government of British Columbia, records classification is combined with information retention scheduling in one integrated system known as Administrative Records Classification System (ARCS) and Operational Records Classification Systems (ORCS).

2.1 Ministries must follow processes set out by the CRO for the development, approval, and implementation of information schedules. For guidance, see RIM 201 Records Schedule Development, Approval and Amendment.

2.2 Ministries must implement and maintain office recordkeeping systems organized in accordance with the Administrative Records Classification System (ARCS), a program-specific Operational Records Classification System (ORCS), and/or other ongoing records schedules (including government-wide Special Schedules). For guidance, see RIM 102 Government Recordkeeping.

2.3 Ministries must apply the retention requirements of applicable information schedules to government information for which they are responsible and ensure appropriate destruction in accordance with section 4 of this policy.

2.4 Archival appraisal of government information must be undertaken by CRO delegates, in accordance with CRO policy and processes.

3. Preservation and Storage

Preservation

Government must preserve information to ensure the integrity of the evidence of its business, meet its legal obligations, and demonstrate accountability.

3.1 Ministries must ensure government information in their custody or control is preserved in a manner that protects authenticity, accessibility and context throughout the information's lifecycle.

3.2 Ministries must maintain and preserve records and data in formats that are stable and accessible in the long-term (i.e. for as long as the applicable information schedule requires). This includes reformatting and moving records and data to new systems when appropriate.

3.3 When digitizing government information other than transitory information, ministries must follow the Digitizing Government Information Standard.

3.4 Ministries must ensure that any data migrations follow corporate policies, standards and procedures, and are documented appropriately.

Storage

3.5 Ministries transferring physical records to offsite storage must use approved records storage facilities and services. For guidance, see RIM 422 Preparing Records for Offsite Storage, Section 2.1: Using Approved Records Storage Facilities.

3.6 Ministries must prepare records for storage in a manner that ensures the records will remain accessible for as long as they are required to support government business and accountability needs.

3.7 Metadata must be persistently linked with information, regardless of where the information is stored over time.

4. Transfer and Disposal

Transfer

4.1 Before transferring custody of any government information to a government body covered by the IMA (including another ministry), ministries must authorize the transfer. For guidance, see RIM 503 Records Transfer within Government.

4.2 Ministries must ensure that the transfer of government information and associated metadata in their custody or control is:

a. undertaken in accordance with corporate policies, standards and procedures; and
b. managed and documented appropriately with due regard for applicable access, confidentiality, and security provisions.

4.3 Ministries must follow CRO processes for alienation of information (i.e., when transferring government information to a non-government agency). For guidance, see RIM 504 Records Transfer Outside of Government.

Government Archives

4.4 Ministries must work with the CRO to ensure that all physical and digital records in their custody or control that are eligible for archival transfer are transferred to the appropriate government archives.

4.5 When preparing government information for transfer to the government archives, ministries must ensure that the records:
   a. maintain their integrity, reliability, security and confidentiality during the transfer process administered by the CRO; and
   b. meet any additional requirements established by the CRO.

Destruction

The IMA requires ministries to dispose of government information in accordance with an applicable information schedule or, if no information schedule applies, only with CRO approval. For guidance, see RIM 501A Specifications for Destroying Records Onsite and RIM 501B Specifications for Destroying Records in Offsite Storage Facilities.

4.6 Ministries must use destruction methods that protect security and confidentiality in compliance with applicable policy and procedures.

4.7 Ministries must suspend destruction of information if a related litigation, legal action, request made under FOIPPA, or investigation is underway or anticipated.

4.8 Ministries must not destroy or alter information (including associated metadata) normally preserved in enterprise government backups except in accordance with approved information schedules and processes.

5. Training and Guidance

Ministries are encouraged to support a culture of responsible IM. As outlined in the Appropriate Use Policy (AUP), supervisors are responsible for ensuring that employees receive the level of training on managing government information that is necessary to perform their duties. In addition:

5.1 Ministries must ensure that IM training is available in each office to ensure that employees are aware of how the office manages its information holdings.

5.2 Ministries must ensure mandatory IM training is completed by employees (e.g., IM 117). For more information on available training, see the GRS Learning Page and the PSA Learning System.

6. Evaluation and Compliance

Ministries' IM practices may be evaluated, audited or reviewed by the CRO, independent offices such as the Auditor General and others with designated authority. In addition to cooperating with external evaluators, auditors or reviewers:

6.1 Ministries must regularly evaluate their management of government information to help determine their IM maturity and compliance with applicable legislation, policies and standards.

ROLES AND RESPONSIBILITIES

Deputy Ministers (or equivalent positions) or delegates

Deputy Ministers (or equivalent positions) or delegates have the responsibility to:

- Ensure that ministry-specific IM resources and training are in place as necessary;
- Oversee the development and implementation of ministry-specific policies, processes and procedures to support IM and adherence to corporate processes, as specified in the Recorded Information Management Manual; and
- Ensure the ministry's information holdings are managed in accordance with applicable legislation, policies, standards and procedures.

Chief Records Officer (CRO)

Further to the mandate set in the IMA and responsibilities outlined in CPPM Chapter 12, the Chief Records Officer (CRO) or delegates have the responsibility to:

- Collaborate with the rest of the OCIO and ministries to develop clear and adequate IM strategies, policies, standards, processes and procedures, including information schedule development and information disposal;
- Provide expert IM guidance in the form of online guides and learning resources, as well as advice and training to help ministries meet their IM obligations;
- Administer government's standard Enterprise Document and Records Management System (EDRMS), and other corporate recordkeeping systems;
- Set standards for offsite records storage facilities, and administer offsite records storage and access on behalf of ministries—this includes managing enterprise contracts for long-term offsite storage of government information by service providers;
- Conduct archival appraisal to determine the retention requirements for government information, including identifying which information will be preserved in the government archives;
- Approve information schedules, or delegate this responsibility as appropriate (e.g., to an established Information Management Advisory Committee);
- Accession government information as appropriate;
- Manage processes for transferring government information to the government archives; and
- Evaluate the management of government information, including ministry IM practices.

DEFINITIONS

Accessibility: The characteristic of being easily reached, retrieved, or used by people regardless of abilities. In the context of IM, accessibility refers to the availability and usability of recorded information. For information on the Province's commitments to building a better B.C. for people with disabilities, please visit https://www2.gov.bc.ca/gov/content/governments/about-the-bc-government/accessibility.

Accession: A body of records registered as a unit (and given an accession number) for the purposes of administrative control. This includes physical identification and control of transfer, storage,

retrieval, and disposition. Accessions typically cover records maintained in a records storage facility contracted by government.

Alienation: The permanent transfer of records, and all rights to and ownership of the records, from ministries to another entity in accordance with the IMA.

Authenticity: The quality of being genuine, not a counterfeit, and free from tampering or corruption. Authenticity alone does not automatically imply that the content of information is reliable or accurate; it merely establishes that information is what it purports to be and has been verified as the original.

Classification: The process of identifying records or information in accordance with a predetermined filing or security system. This includes determination of the function and/or subject of a record and selection of the appropriate classification for filing.

Critical information: The records and data essential to the operations of a government business area. This includes information that supports business continuity by documenting and supporting core programs, functions, responsibilities and commitments (e.g., security and risk mitigation information, records needed to meet financial and legal requirements). Critical information also includes information of public interest and permanent value.

Data: The smallest meaningful units of recorded information generated by an organization, which gain significance when stored in a structured manner that enables them to be synthesized and interpreted.

Digital archives: As defined in Part 1 of the IMA.

Disposition: The process which enables government to dispose of records which no longer have operational value, either by permitting their destruction, by requiring their transfer to the government archives, or by agreeing to their alienation from control of government.

Employee: An individual working for, or on behalf of, a ministry, agency, board or commission subject to the Core Policy and Procedures Manual.

Government archives: The entirety of government information assets that have been appraised as having permanent value to government and society and are preserved and made publicly accessible. Government's physical archival records are held by the Royal British Columbia Museum. The CRO is responsible for government's digital archival holdings.

Government information: As defined in Part 1 of the IMA. Can include both data and records.

Information: Any collection of data that is processed, analyzed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form.

Information management (IM): The means by which an organization plans, collects, organizes, governs, protects, uses, controls, disseminates, exchanges, maintains and disposes of its information; as well as any means through which the organization ensures its information's value is identified and that the information is used to its fullest extent, including the facilitation of efficient discoverability of information.

Information schedule: Approved by the CRO under the IMA, an information schedule provides a timetable that governs the lifecycle of government information. Information schedules specify how records are managed to ensure that government information is kept for as long as required and authorize the holding, transfer and disposal of records.

Integrity: The quality of being whole and unaltered through loss, tampering, or corruption. In the context of records, integrity relates to the potential loss of physical or intellectual elements after a record has been created. As one of the components used to determine a record's authenticity, integrity is a relative concept that assesses whether the essential nature of a record has changed.

Lifecycle: The lifespan of information from its creation or receipt and use, through to its final disposition: destruction, transfer to the government archives or alienation.

Office of primary responsibility (OPR): The office that has primary responsibility for a category of records or holds the master/official file copy of any record series for that ministry or agency. The OPR maintains the official master copy of the records in order to satisfy operational, financial, legal, audit and other requirements.

Preservation: The principles, policies, rules, strategies, and activities aimed at prolonging the existence of an object by maintaining it in a condition suitable for use, either in its original format or in a more persistent format, while leaving intact the object's intellectual form.

Record: Information created, received and maintained by an organization or person, in pursuance of legal obligations or in the transaction of business. This includes records formats defined in the *Interpretation Act* and FOIPPA.

Records management: The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (Source: ISO 15489, cited in International Council on Archives).

Reliability: In the context of the records management discipline, relates to the trustworthiness of a record as a statement of fact; a record's ability to serve as reliable evidence. Reliability is established by examining the completeness of the record's form and the amount of control exercised on the process of its creation.

Service provider: A person retained under a contract or service agreement to perform services for a ministry, agency, board or commission subject to the Core Policy and Procedures Manual.

Supervisor: A person to whom an employee directly reports or a person who manages a service provider contract or service agreement.

Transitory information: Information of temporary and/or low value that is needed for only a limited period of time in order to complete a routine action or prepare a subsequent record (e.g., a new version). For more information, see the Transitory Records Guide.

REVISION HISTORY

Version	Date	Notes
1.0	June 19, 2020	Approved by the Chief Records Officer (CRO) May 25, 2020; date of issue June 19, 2020