Managing Information in Ministers' Offices

October 2019

Alberta

Agenda

Introduction

Information Management – Records

Safeguarding Government Information

Introduction

Information is one of the Government's most valuable assets. All Public Service (APS) employees have a responsibility to take reasonable steps to safeguard it, regardless of whether they are the creator or recipient of the information.

Information Management - Records

Relevant Acts and Legislation

Government information is managed in accordance with:

1. **Records Management Regulation (RMR)**

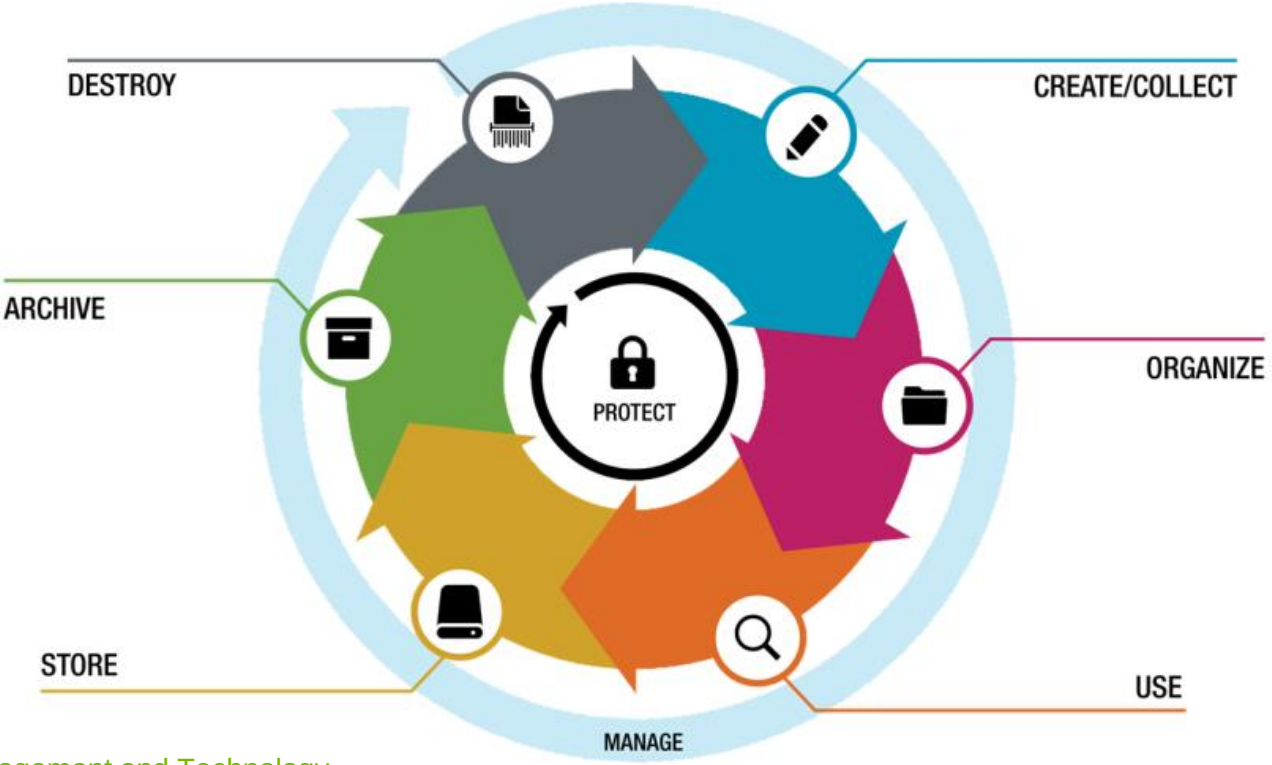
2. ***Freedom of Information and Protection of Privacy (FOIP) Act***

Records in the GoA

In the Government of Alberta (GoA), the *FOIP Act* defines "record" as a record of information in **any form**.

Government records are records in the custody or under the control of government organizations and must be retained and managed appropriately.

Information Management Lifecycle



Creating/collecting information

Information is required to be created and collected to document and provide evidence of business decisions and transactions and to maintain corporate memory.

Applying security classification

Public	Applies to data and information that, if compromised, **will not** result in injury to individuals, governments or to private sector institutions.
Protected A	Applies to data and information that, if compromised, **could cause** injury to an individual, organization or government.
Protected B	Applies to data and information that, if compromised, **could cause serious** injury to an individual, organization or government.
Protected C	Applies to data and information that, if compromised, could **cause extremely grave** injury to an individual, organization or government.

The applied classification level is not static and can change in any direction, in any order, and at any time.

Alberta

Organizing Minister’s office records

Each type of record in the Minister’s office has specific records management requirements and must be managed separately.

Types of records in Ministers' offices

Government Records

Departmental: related to the mandate of the department

- Specific program policy, annual reports, minister's expense claims

Cabinet: related to cabinet committees and sub-committees

- Approval of government policy, recommendation for approval of Orders in Council

Other Records

Constituency: created and received as an MLA

- Election campaigns, constituency business

Personal: created and received as a private citizen

- Home electric bill, association membership receipt, email to family members.

Alberta

Using and Storing Minister's office records

Type of record	Use/storage requirements
Departmental	The Minister's office only retains departmental records needed for current business and returns them to the department when no longer needed.
Cabinet	Executive Council is the official custodian of the master set of Cabinet records.
Constituency and personal	The Minister is responsible for managing how these records can be used and stored.

Disposing of Minister's office records

Type of record	Disposition requirements (Must be disposed of..)
Departmental	According to the retention schedule for that business area.
Cabinet	Under the Minister's records schedule (2002/041).
Constituency	Contact the Legislative Assembly Office Senior Records Officer for guidance on disposition.
Personal	Minister may keep them, destroy them or donate them to the Provincial Archives of Alberta.
Transitory	Regularly in accordance with the Transitory Records Retention and Disposition Schedule (1995/007-A0001).

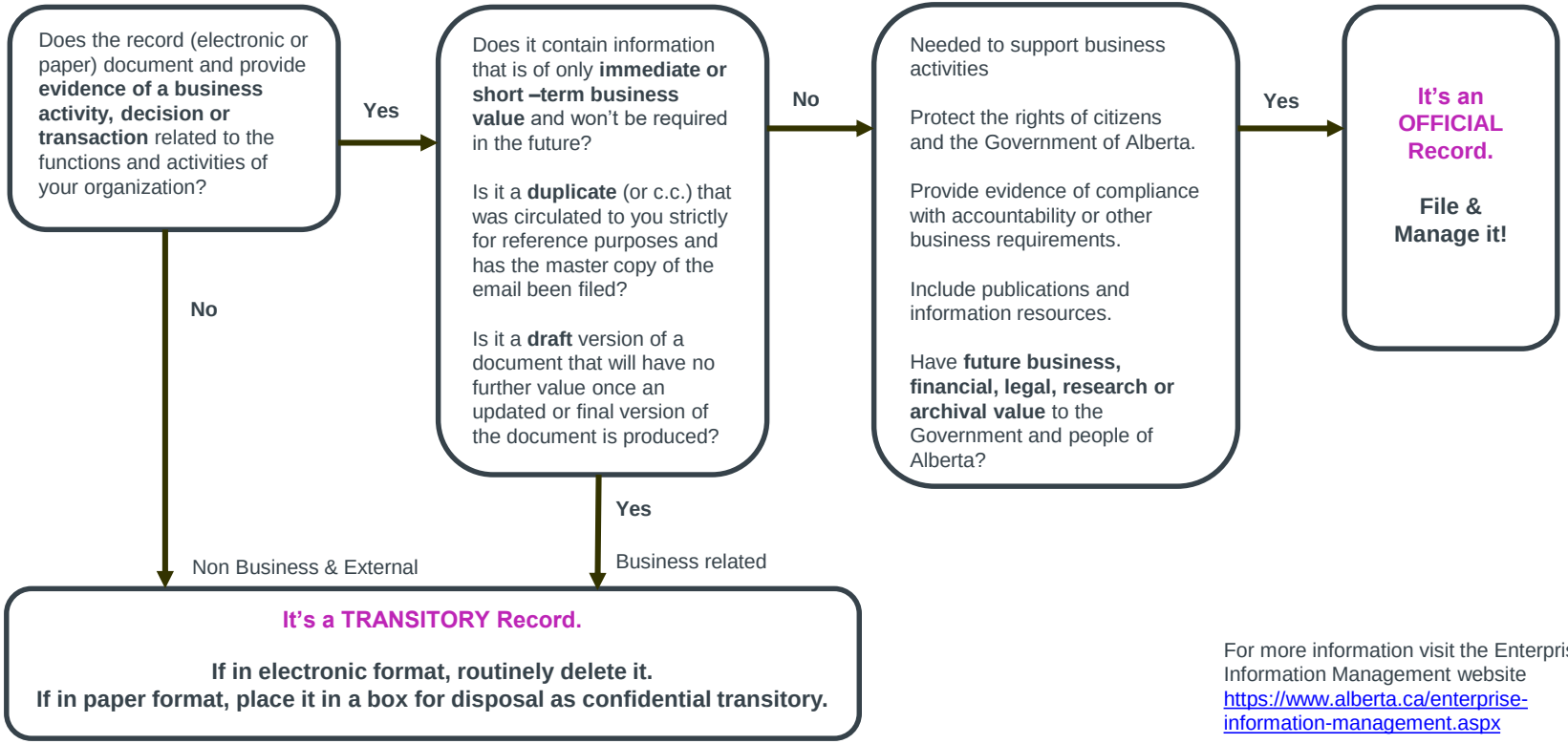
Transitory records

Transitory records have no further value to government beyond an immediate or minor transaction.

These records provide no evidence of business transactions and no future value (legal, financial, operational, archival).

Transitory Records

What to Dispose of and What to Keep and Manage



For more information visit the Enterprise Information Management website https://www.alberta.ca/enterprise-information-management.aspx

Exceptions to disposition

Information that has, or is reasonably anticipated to have, a legal or FOIP hold cannot be disposed of until the holds have been resolved.

For more information on the types of information protected by the *FOIP Act* please contact your FOIP Coordinator after discussing with your supervisor.

Safeguarding Government Information

Protecting information

Throughout the information management lifecycle, information must not only be managed but it must be protected to ensure they are only accessed by those who are authorized to do so.

Note: All Cabinet related records will be shared and stored using the Secure Document Solution and/or eCommittee.

Corporate Information Security Office (CISO)

CISO ensures the confidentiality, integrity and availability of the GoA's information and technology assets. CISO's activities enable the GoA to operate securely and meet its digital service delivery commitments to the people of Alberta.

Three Key Cyber Security Protections

The GoA has a Cyber Security Strategy for protecting, detecting, managing, and responding to cyber threats, as well as recovering from any related disaster events:

IT security services

- monitoring and first response for the GoA network 24x7, block unnecessary or unauthorized network traffic coming from outside of North America

IT and software support

- using strong passwords, access controls for files, services and system to prevent, detect, and manage cyber attacks or identified malware

Proactive prevention

- online training for information management, information security, and privacy, IMT risk management, and IT disaster recovery plan testing

Alberta

Physical security – access

- Wear your employee identification in plain view at all times
- Politely ask people you do not know if you can help them (if you are comfortable doing so)
- Do not let people follow you through access points if you do not know them
- Report doors that do not close properly to your supervisor or building security
- Report security pass issues (e.g. unreturned security passes)

Physical security – at your workspace

- Lock your computer when you leave your desk
- Secure sensitive documents and portable storage devices in a locked desk or filing cabinet
- Set up a PIN to hold sensitive print jobs until you can pick them up

Clean desk responsibilities

- Clear desks, work stations/surfaces, etc. of all government information at the end of each day, and secure the materials in provided storage spaces
- Take reasonable steps to safeguard APS-issued IT assets and sensitive information
- Report any actual or suspected information security and privacy breaches to your supervisor, CISO (if a security breach), and your FOIP contact (if a personal information breach) immediately

Outside the workplace

- Do not forward government information to personal accounts
- If you require materials that are not accessible digitally (such as paper based sensitive information), record their removal from the workplace
- Give serious consideration before printing and always ensure you properly protect and dispose
- When using remote access services, avoid public Wi-Fi and ensure you are the only one using your government device

International Business Travel

Avoid connecting to Public Wi-Fi in hotels, cafes, or other public places – if you must connect, use VPN or other secure mechanism.

Consider the security of your device and its content, and be mindful of your surroundings – if you must store sensitive documents on your device, ensure that they are removed as soon as no longer needed.

Always be suspicious of emails and documents you get from unknown sources – Do not open suspicious emails or attachments, and don't click on website links unless you know where they will lead you.

Delete browser history, caches, cookies after using the internet on public systems.

Do not accept gifts of USB sticks or allow portable storage devices to be plugged into your device.

Maintaining confidentiality

Alberta Public Service Oath of Office

- Confirms that you will maintain the confidentiality of information or documents that come into your possession or you have knowledge of in your role as public servant.

Code of Conduct

- Understanding if there is a conflict of interest between your private interests and your APS duties.
- Employees who speak or write publically shall ensure that they do not release information in contravention of the Oath of Office.

Storing sensitive records

Sensitive, paper-based information should be stored in lockable file cabinets in a physically secure, supervised area not accessible by the public.

Digital records are to be stored in approved GoA secure repositories, not on removable devices, personal drives, or personal cloud storage.

Social engineering

A popular type is email phishing. Attempts to trick employees into disclosing personal or sensitive information.

Red flags include:

- Hyperlinks that look unusual or contain a non-corporate address
- Request is not typical or out of the ordinary of the sender
- Formatting of the email appears to be authentic
- Email is written to convey a sense of urgency

Protect your passphrases

Common best practices for creating secure passphrases:

- Choose passphrases that you will remember, but would be hard for others to guess.
- Replace parts of your phrase with letters, numbers or special characters (including spaces).
  - Example: Br1ng me Maple syrup

Information management contacts

- Sector Chief Information Officer (SCIO)

  https://occio.gov.ab.ca/imtgovernance/SitePages/About%20the%20Transformation.aspx

  Note: each Sector has an Information Management (IM) Director and IM Associate Director
- Information Management Professionals

  https://www.alberta.ca/assets/documents/IM-SRO-List.pdf
- Sector Information Security Officers

  http://www.servicelink.gov.ab.ca/security/MinistryInformationSecurityOfficers.cfm
- Enterprise Information Management Branch

  SA.InformationManagement@gov.ab.ca
- Corporate Information Security Office

  ciso@gov.ab.ca

Tools and Resources: Training

Online training modules available to GoA employees through the Learning Management System (LMS) http://goalms.alberta.ca

- Information Management
- Cyber Security
- Physical Security

Tools and Resources: Guidance

- Official and Transitory Records: A Guide for Government of Alberta Employees

  https://www.alberta.ca/assets/documents/IM-Transitory-Records-Guide.pdf
- Official and Transitory Records Flowchart

  https://www.alberta.ca/assets/documents/IM-Transitory-Records-Chart.pdf

Tools and Resources: Schedules

- Transitory Records Schedule (1995-007-A001)

  https://www.alberta.ca/assets/documents/IM-Schedule-1995-007-A001.pdf

- Minister's Records Schedule (2002/041)

  https://www.alberta.ca/assets/documents/im-schedule-2002-04-A001.PDF

Tools and Resources: Related websites

Freedom of Information and Protection of Privacy Act

http://foip.alberta.ca

Personal Information Protection Act

http://pipa.alberta.ca

Information management resources

https://www.alberta.ca/enterprise-information-management.aspx

Corporate Information Security Office

http://www.servicelink.gov.ab.ca/security/

PAA Guide to Personal and Family Records

http://provincialarchives.alberta.ca/docs/family-histories-april-2018.pdf

Questions?