Safeguarding Government

Information

Alberta

Service Alberta, Government of Alberta
August 2021
Safeguarding Government Information

Overview

Information is one of the Government's most valuable assets. All Alberta 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. Safeguards have been established to ensure sensitive information is only accessed by those that are authorized to do so, reducing risk to Albertans and the Government. This guide has been created to assist APS employees in securing:

- their workplace; and
- the information (sometimes referred to as data, documents, records, content) they create and manage on behalf of the people of Alberta.

This guide is the result of collaboration between:

- Corporate Information Security Office (CISO);
- Enterprise Information Management (EIM);
- Freedom of Information and Protection of Privacy (FOIP) Division; and
- Public Service Commission (PSC).

By consistently practicing a few simple habits, APS employees can ensure sensitive information is safeguarded.

Basic Do's and Don'ts

- Remember your Oath of Office as a member of the APS. Do not disclose government information, regardless of its sensitivity, without appropriate authorization.
- Maintain a "clean desk" and always lock your computer (Windows Key + L) when you are away from your desk.
- Use the provided locked bins whenever you are disposing of any transitory physical information. Do not dispose of government information in recycling containers.
- Do not discuss or review sensitive government information in open work spaces, public areas, or when using public Wi-Fi.

To do:

Refresh your awareness on the Code of Conduct and Ethics for the Public Service of Alberta and the Oath of Office.

At the Workplace

Access

Security starts at the front door. Managing who gets into your workplace is an essential safeguard for government information. Follow these simple practices to prevent unauthorized access:

- Wear your employee identification in plain view at all times. This makes people who are not wearing them more visible.
- If you see someone you do not know in your area or waiting at an access point, politely ask if you can help (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., access to areas that should be off limits, unreturned security passes).

To do:

Any physical security concerns should be immediately reported to your supervisor and building security.

At Your Workspace

Developing and implementing security-conscious work habits will reduce the likelihood of someone seeing or disclosing sensitive information. Regardless of where you work (e.g., dedicated office, hoteling station, home, etc.) your practices should include:

- Locking your computer when you leave your desk to prevent unauthorized users from accessing the government network and/or information.
- Securing sensitive documents and portable storage devices in a locked desk or filing cabinet.
- Setting up a PIN code to hold sensitive print jobs until you can pick them up. Contact the Government of Alberta (GoA) Help Desk if you need assistance setting up secure print capabilities.

Clean Desk Responsibilities

Employees (which includes all staff levels, contractors, volunteers, appointees and students working with a public body) are expected to take reasonable steps to ensure the security of government information they are creating or that is in their custody. Remember to clear desks, work stations or work surfaces and secure all information prior to leaving the work area unattended. If you work in a space with unassigned seating (e.g., flex spaces or hoteling stations), use the storage spaces provided. All APS employees have a role to play in safeguarding information:

Executive Directors and Directors

- Ensure employees have adequate facilities to safeguard government information.
- Communicate procedures for the security of government information within your branch.

Managers and Team Leads

- Provide suitable and sufficient lockable containers/filing cabinets for employees.
- Advise employees of their responsibility to secure materials at the end of each workday.
- Monitor employee compliance of clean desk practices.

Employees

- 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 (in the case of a security breach), and your FOIP contact (in the case of a personal information breach) immediately.

Note:

All APS employees are obligated to ensure documents are secure throughout the information management lifecycle (i.e., creation, use, disposal).

Outside the Workplace

Secure Remote Access Services (Citrix, VPN, etc.) are provided upon request to ensure a secure connection to the GoA network when working remotely. Once connected, you will be able to access the same network resources (e.g., file shares) the way you normally would in an APS office.

To ensure that your information remains secure outside the workplace, take the following steps:

- Government information is not to be created, sent, forwarded, or received through personal accounts (e.g., Dropbox, Gmail, Hotmail, Yahoo Mail, Google Drive, OneDrive, Dropbox, etc.).
    - Use only government-issued devices (laptops, smartphones, USB keys, etc.) or approved multi-factor authentication methods of logging in remotely from a personal device (e.g., Citrix) for government work and for remote access to the GoA network. Government-issued devices offer security features, such as encryption, password protection, and the ability to be wiped remotely if lost or stolen.
- Do not store or transport sensitive information on mobile devices. If an exception is required, please speak to your supervisor.
- If you need materials that are not accessible digitally (such as paper based sensitive information), record their removal from the workplace.
    - Removed materials are to be returned to the workplace as soon as possible. Record that the materials have been returned and share this information with your manager.
- When using remote access services, avoid public Wi-Fi and ensure that you are the only one who works on your government computer. Safeguard sensitive information while in transit or outside the office.

Online training is available for information management, privacy and security at: https://goa.noverant.com

Do not:

Leave mobile devices or sensitive documents unattended or in plain view (e.g., in the backseat of your car, gym locker rooms, etc.).

Maintaining Confidentiality

The APS aspires to uphold the highest standards in maintaining confidentiality and professional integrity.

All APS employees are required to swear or affirm an Oath of Office and an Oath of Allegiance upon appointment to the APS. The 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 a public servant.

Alberta Public Service Oath of Office

"I, , do swear that I will execute according to law and to the best of my ability the duties required of me as an employee in the public service of Alberta and that I will not, without due authorization, disclose or make known any matter or thing which comes to my knowledge by reason of my employment in the public service"
Source – *Public Service Act*

To do:

Remember your Oath of Office. Do not discuss sensitive information with co-workers or stakeholders unless authorized.

Code of Conduct

The Code of Conduct can help you recognize when there may be a conflict of interest between your private interests and your APS duties. Employees are required to disclose any situation which is, or appears to be, a conflict of interest.

There are two sections of the Code of Conduct which specifically address confidentiality of information:

- **Section 8. Furthering Private Interests** - Employees are in conflict of interest and in violation of the Code of Conduct if they use or communicate information not available to the general public that was gained by the employee in the course of carrying out their duties.
- **Section 16. Public Statements** – Employees who speak or write publically shall ensure that they do not release information in contravention of the Oath of Office. This responsibility for maintaining the confidentiality of information or documents includes the responsibility for ensuring that such information or documents are not directly or indirectly made available to unauthorized persons.

The GoA requires strict confidentiality on all sensitive information (e.g., material going to Treasury Board and Cabinet for consideration). Employees may not directly or indirectly release information, regardless of its sensitivity, unless they are expressly authorized to do so.

Importance of Confidentiality

Confidentiality

- Recognizes the right of every Government to consider in confidence a wide range of advice and options, have open and frank discussions before making a collective decision, and decide when to make those decisions public.
- Protects the relationship of trust that is necessary for an effective working relationship between the public service and the Government.
- Protects sensitive information that is often accessible to public servants as part of their work, including personal information.
- Protects the legal and commercial interests of the Government and affected stakeholders by ensuring information is disclosed to all interested parties in a planned and coordinated manner, avoiding unfair advantage to those receiving unauthorized confidential information and preventing breaches of notification requirements in existing agreements.

Handling Sensitive Information

Classifying Information

All APS employees have a responsibility to take reasonable steps to safeguard information, regardless of whether they are the creator or recipient of the information, and manage it according to the Data and Information Security Classification Standard and guides.

Employees must:

- Label all records with the correct security classification level;
- Safeguard the information accordingly; and
- Recognize the security levels assigned to government information created by others and safeguard those assets accordingly.

If you have questions about which security classification to apply to information you have created or received, speak with your supervisor.

Security classification labels, which are based on the sensitivity of the information, are a mandatory GoA safeguard. Sensitive information (i.e., personal information, advice in briefing notes, Cabinet confidences, etc.) must be labelled at the time it is created or collected. Labelling is used to signal that information requires special handling and indicates the requirement for increased safeguards.

Below is a scenario that highlights the fluidity of security classification as a policy moves through development. From initial conceptualization to a final published form, the applied security classification will change:

- An initial draft of a policy could be **Protected A**; **Protected B** or **Protected C**, depending on the context of the policy or its intended use.
- Consultations for a draft policy may be **Public** (if there is a public consultation), **Protected A** (if there is an internal government consultation), or **Protected B** (if there is a confidential consultation with external stakeholders).
- Analysis of potential policy options based on consultation may be **Protected A** or **Protected B**, and Cabinet deliberations may be **Protected B** or **Protected C**.
- Published policy and accompanying guidance will have the security classification of **Public**, but policy interpretations may have the security classification of **Protected A** or **Protected B**.

Consultation and collaboration with relevant stakeholders will result in the selection of an appropriate security classification. After the security classification has been decided, it may be applied to:

- the system and/or application in which the data or information is maintained;
- an individual record; or
- a field within a system and/or application.

Security Classification	Definition	Examples of Typical Safeguards	Document Examples
Public	Applies to data and information that, if compromised, will not result in injury to individuals, governments or to private sector institutions.	• Apply security classification label (e.g., header/footer, naming convention, subject line, stamp, metadata, etc.). • No special storage requirements, but must be stored in approved GoA repositories. • No special procedures for transmission.	Press release.
Protected A	Applies to data and information that, if compromised, could cause injury to an individual, organization or government.	• Apply security classification label. • Store in a secure location (e.g., locked desk drawer or cabinet) when not in use. • Provided locked bins are to be used to discard physical copies that have been identified as transitory. • Logical access controls in place (e.g., group authorized access).	User manual for a government system or application.
Protected B	Applies to data and information that, if compromised, could cause serious injury to an individual, organization or government.	• Apply security classification label. • Store in a secure location (e.g., locked desk drawer or cabinet) when not in use. • Users require additional authentication credentials to gain access (e.g., user name and password) that are auditable. • Provided locked bins are to be used to discard physical copies that have been identified as transitory.	A briefing note containing industrial trade secrets.

Security Classification	Definition	Examples of Typical Safeguards	Document Examples
Protected C	Applies to data and information that, if compromised, could cause extremely grave injury.	• Apply security classification label. • Transmitted and stored in highly secure ways (e.g., audit trails of continuous chain of custody, encryption). • Enhanced access controls in place (e.g., authorized individuals only). • Provided locked bins are to be used to discard physical copies.	Meeting minutes regarding a child in protective custody.

If you have questions about which security classification to apply to information you have created or received speak with your supervisor. For an example of an applied security classification label, please see the footer below.

Reclassifying Information

Information may be reclassified at any point in its lifecycle. For example, before the provincial budget is released, a draft news release about the budget document would likely be considered "Protected B" the day before it is released. However, once published, the published news release is then considered "Public".

Information Received from Other Jurisdictions

Information that has been received from another jurisdiction must:

- maintain the classification level applied by the originating jurisdiction; and
- be handled according to the rules and procedures established by the originating jurisdiction.

If the information received from another jurisdiction lacks security classification, it is subject to the GoA Data and Information Security Classification Standard, and must be properly assessed and classified in collaboration with the originating jurisdiction.

To do:

Apply information security classification labels, as they communicate requirements for special handling to protect the information's confidentiality, integrity and availability based on its sensitivity.

Storage

Sensitive, paper-based information should be stored in lockable file cabinets (particularly if they are original documents) in a physically secure, supervised area not accessible by the public.

Digital records are to be stored in approved GoA secure digital repositories, not on personal drives. The use of systems and/or applications that have been designed for the storage of sensitive information is an essential safeguard to ensure the information is not accessed by those that are not authorized to do so.

Note:

The Secure Document Solution is to be used for highly sensitive documents (e.g., sensitive Action Requests relating to Cabinet, Treasury Board Secretariat, and Advice to Premier, and Premier decision documents) – templates are also available in the Secure Document SharePoint.

Disposition

Information, regardless of its format, must be disposed of in accordance with approved records retention and disposition schedules, which are legal authorities that specify how long records are to be kept, and their final disposition (destruction or archival preservation). Some information that APS employees receive may be considered transitory, and should be handled accordingly; please consult the following resources for additional guidance:

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

Note:

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.

To do:

Refer to the Resources/Links section at the end of this document for additional training and guidance on how to appropriately classify, handle, store, and dispose of sensitive information.

APS employees regularly dispose of transitory information, either by deleting transitory digital documents or discarding transitory paper documents in confidential receptacles or locked bins.

Communicating Sensitive Information

The below scenarios capture appropriate safeguards being taken to ensure information is not inappropriately disclosed.

Email

Avoid using an email to distribute highly sensitivity information. Instead, use systems designed with the purpose of safeguarding sensitive information. If email must be used, appropriate safeguards (e.g., encryption) must be applied. In addition:

- Double-check the recipient list before hitting send.
- Ensure you identify the security classification level of emails by including the label in the subject line.

Telephone

If you are contacted by an unknown caller, record their number and question and then talk to your supervisor before providing a response. These calls may need to be directed to a:

- Ministry general information line; or
- A media relations contact.

Corporate Information Security Office (CISO)

The role of the CISO is to ensure 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.

Phishing

Phishing is a threat to information security and personal information where an attacker contacts someone by email, in an attempt to trick them into disclosing personal or confidential information. A phishing email may be very simplistic, or it may be crafted to appear like an email from a trusted source, such as a business, bank or friend.

Red Flags

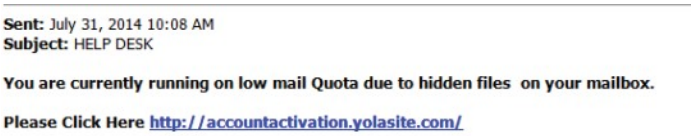
- Hyperlinks - Look for web addresses in hyperlinks that look unusual or contain a non-corporate address.
    - Government addresses will include gov.ab.ca, or alberta.ca. Hovering the mouse pointer over the link will display the hyperlink address if it is hidden.
- Atypical Request - The type of request received from the sender is not typical or is out of the ordinary.
    - Formatting the email to include correspondence from the "Help Desk" is a common tactic used to authenticate the email.
- Appearance - Phishing emails are formatted to appear authentic by containing logos, addresses, or names that look official.
    - It is common for an email to take the form of a bank notice regarding a customer's account, or from the Help Desk requesting a software update or password change.
- Urgency - Usually the emails are written to convey a sense of urgency.
    - The attacker may also spend time personalizing emails by including specific information about the recipient. This technique is known as "Spear Phishing", and the email may disclose personal details such as the individual's address, account number or previous transactions.

Example:

To do:

Only open emails you trust. Be careful if you receive an email from an unfamiliar source. Learn more about possible phishing threats through the Phishing Tip Sheet.

The above example contains:



Sent: July 31, 2014 10:08 AM
Subject: HELP DESK

You are currently running on low mail Quota due to hidden files on your mailbox.

Please Click Here http://accountactivation.yolasite.com/

- Minimal details about the request;
- Conveys a sense of urgency; and
- Provides a hyperlink that is not a Government website.

How to Handle Potential Phishing Attacks

If anything within a received email raises suspicion (even if it seems minor to you), err on the side of caution and:

- Do not click on any of the hyperlinks in the email; and
- Immediately contact the Service Desk or your Sector Information Security Officer.

Cyber Security

These resources should be consulted by all APS employees to help build cyber resilience:

- Cyber Security Learning Centre
- Information management, privacy and security: https://goa.noverant.com

Protect Your Passphrases

User IDs and passphrases must not be divulged to anyone, for any reason. You are accountable for all APS IT assets (e.g., computing devices, passphrases, etc.) you use.

Common best practices for passphrases include:

- Choose passphrases that you will remember, but would be hard for others to guess.
- Replace parts of your phrase with letters with numbers or special characters (e.g., “Say hello to my friend” can be $Aye!!02myF).

For additional guidance, please refer to the following tip sheet: Passwords and Passphrases

Remember

To do:

- Refresh your awareness on the Code of Conduct and Ethics for the Public Service of Alberta and the Oath of Office.
- Any physical security concerns should be immediately reported to your supervisor and building security.
- Remember your Oath of Office. Do not discuss sensitive information with co-workers or stakeholders unless authorized.
- Apply information security classification labels, as they communicate requirements for special handling to protect the information's confidentiality, integrity and availability based on its sensitivity.
- Refer to the Resources/Links section at the end of this document for additional training and guidance on how to appropriately classify, handle, store, and dispose of sensitive information.
- Only open emails you trust. Be careful if you receive an email from an unfamiliar source. Learn more about possible phishing threats through the Phishing Tip Sheet.

Note:

All APS employees are obligated to ensure documents are secure throughout the information management lifecycle (i.e. creation, use, disposal).

- The Secure Document SharePoint is to be used for highly sensitive documents (e.g., sensitive Action Requests relating to Cabinet, Treasury Board Secretariat, and Advice to Premier, and Premier decision documents) – templates are also available in the Secure Document SharePoint.
- 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.

Do not:

- Leave mobile devices or sensitive documents unattended or in plain view (e.g., in the backseat of your car, gym locker rooms, etc.).

Resources/Links

Legislation

- Code of Conduct and Ethics for the Public Service of Alberta
  - https://open.alberta.ca/publications/code-of-conduct-and-ethics-for-the-public-service-of-alberta
- *Freedom of Information and Protection of Privacy Act*
  - https://www.servicealberta.ca/foip/legislation/foip-act.cfm
- *Oaths of Office Act*
  - http://www.qp.alberta.ca/documents/Acts/O01.pdf
- *Public Service Act*
  - http://www.qp.alberta.ca/documents/Acts/p42.pdf
- Records Management Regulation
  - http://www.qp.alberta.ca/documents/Regs/2001_224.pdf

Information Disclosure Policies

- Communications Policy
  - https://open.alberta.ca/publications/9781460141120
- Social Media Policy
  - https://open.alberta.ca/publications/government-of-alberta-social-media-policy

Data and Information Security Classification

- Data and Information Security Classification Standard
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Data-and-Information-Security-Classification-Standard.pdf
- Data and Information Security Classification Guideline
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Data-and-Information-Security-Classification-Guideline.pdf
- Technical Guide: Labelling Data and Information
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Technical-Guide_Labeling-Data-and-Information.pdf
- Technical Guide: Storing Data and Information
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Technical-Guide_Storing-Data-and-Information.pdf

- Technical Guide: Transmitting Data and Information
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Technical-Guide_Transmitting-Data-and-Information.pdf
- Technical Guide: Appropriate Access to Data and Information
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Technical-Guide_Appropriate-Access-to-Data-and-Information.pdf
- GoA Physical Information Storage Facilities
  - https://imtpolicy.sp.alberta.ca/standards/pdf/Government-of-Alberta_Storage-Facilities.pdf

Disposing of Information

- Official and Transitory Records: A Guide for Government of Alberta Employees
  - https://imtpolicy.sp.alberta.ca/guidelines/Pages/Official-and-Transitory-Records-A-Guide-for-Government-of-Alberta-Employees.aspx
- Official and Transitory Records Flowchart
  - https://imtpolicy.sp.alberta.ca/guidelines/Pages/Official-and-Transitory-Records-Flowchart.aspx

Tip Sheets

- Passwords and Passphrases
  - http://www.servicelink.gov.ab.ca/security/UnsecurePasswords.cfm
- Phishing Tip Sheet
  - http://www.servicelink.gov.ab.ca/security/docs/Phishing_Tip_Sheet.pdf

Training

- Cyber Security Learning Centre
  - http://www.servicelink.gov.ab.ca/security/CyberSecurityLearningCentre.cfm
- Access and Privacy
  - https://www.servicealberta.ca/foip/training-for-public-bodies.cfm
- What is Information Management?
  - http://www.servicealberta.ca/im_ecourse/module1/story_html5.html?lms=1
- How to Manage Information
  - http://www.servicealberta.ca/im_ecourse/module2/story_html5.html?lms=1
- Benefits of Information Management
  - http://www.servicealberta.ca/im_ecourse/module3/story_html5.html?lms=1

Contacts

If you encounter any difficulties with what has been outlined in this guide, or if you wish report a security incident, please refer to the table below.

Website	When to Contact	Email	Phone
CISO http://www.servicelink.gov.ab.ca/security/	To report a security breach.	CISO@gov.ab.ca	From Edmonton: 780-427-1462 Long Distance: 1-800-427-1462
EIM https://www.alberta.ca/enterprise-information-management.aspx	If you have general inquiries on how to manage government information.	SA.InformationManagement@gov.ab.ca	780-427-3884
FOIP https://www.servicealberta.ca/foip/index.cfm	To report a personal information breach.	SA.accessandprivacy@gov.ab.ca	780-427-5848
GoA Service Desk http://webchat.alberta.ca/	If you need technical assistance (e.g., setting up secure print capabilities) or potential phishing attacks.	GoA.ServiceDesk@gov.ab.ca	780-427-1462
PSC https://www.alberta.ca/public-service-commission.aspx	If you questions about the Code of Conduct or the Oath of Office.	psc.erservices@gov.ab.ca	From Alberta: 310-0000 Long Distance: 780-427-2711