Acceptable Use of GoA Information Management and Technology Assets Directive

Cybersecurity Division

Version: 1.0

Approved by: Assistant Deputy Minister and Chief Information Security Officer, Cybersecurity Division	**Owner:** Assistant Deputy Minister and Chief Information Security Officer, Cybersecurity Division	
Approval date: August 8, 2022	**Last Reviewed:** May 3, 2023	**Next review date:** November 1, 2024
Contact: cybersecurity@gov.ab.ca	**Policy Instrument type:** Directive	

Contents

Background 3
Authority 3
Scope 3
Guiding Principles 3
Directive Specification 4
Definitions 6
Roles and Responsibilities 7
Compliance 8
References and Supporting Resources 8
Appendix 1: Guidelines for Acceptable and Unacceptable Activities 9

Background

The Government of Alberta (GoA) owns the data and information that it collects, processes, stores, transmits and receives. The GoA provides employees with business tools, applications and services that assist in meeting GoA business requirements for sharing information and data, enabling collaboration between departments and the public. GoA employees are provided the access required to perform tasks on behalf of Albertans, and are therefore responsible for managing the information and data on behalf of the GoA.

Internal and external threats in a constantly evolving technology landscape present significant risk to the GoA and noncompliance with this directive could result in negative and severe outcomes for the Government and citizens of Alberta. The GoA requires that all Information technology tools be used ethically, responsibly, and in compliance with all legislation and government directives, policies and standards.

This directive cannot anticipate every situation that might arise and does not relieve GoA users from their obligation to exercise common sense. It is everyone's job to protect the integrity and security of the Government of Alberta IMT assets.

Authority

This directive is issued under the authority of the Information Management and Technology (IMT) Policy.

Scope

This directive applies to all GoA staff (which includes, but is not limited to, employees, contractors, volunteers, appointees, interns, and students) covered in the *Public Service Act,* who are provided access to GoA IT assets.

Guiding Principles

- Users are provided with access to GoA IT assets to conduct government business and deliver programs and services to the people of Alberta.
- Users must ensure the use of GoA IT assets is appropriate, lawful and complies with all applicable government and department policies, the Code of Conduct and Ethics for the Alberta Public Service and the Oath of Office (Public Service Act Section 20).
- Users must act to maintain the security and integrity of GoA IT assets and be up to date with their knowledge of security issues by completing cybersecurity awareness training suitable for their role annually.

Directive Specification

1. **Acceptable use of GoA IT Assets**: GoA IT assets include, but are not limited to, physical equipment, such as desktop/laptop/tablet computers, servers, printers, mobile devices, and removable media (such as USB flash drives), as well as GoA services such as networks and cloud. All devices, systems, and data including any personal content stored on government systems are the property of the GoA and all use must be in accordance with this directive, GoA policies, standards, and guidelines. The GoA allows limited use of IT assets for personal reasons (personal correspondence, online banking, etc.).

   Personal use is acceptable if it does not:

   1.1. Negatively impact overall employee productivity;

   1.2. Cause additional expense to the government;

   1.3. Compromise the interests, reputation, or security of the GoA in any way;

   1.4. Disrupt network performance; or

   1.5. Contradict any other GoA policy.

2. **Acceptable use of GoA collaboration tools, services and internet:** The use of GoA collaboration technology, services (including email, instant messaging, forums, and social media), and internet is provided to perform regular job duties as per the following requirements:

   2.1. Users must use the collaboration tools, services and internet in a manner as described in applicable legislation and regulations including privacy legislation as well as the Official Oath of Office, the Code of Conduct and Ethics for the Public Service of Alberta, Respectful Workplace Policy and any applicable supplementary codes;

   2.2. GoA-authorized applications for email, chat and collaboration tools must be used for conducting GoA business both inside and outside of the GoA. Additional collaboration tools may be required to support projects or activities with third parties and may be used provided Cybersecurity Division has completed a risk assessment and the sponsoring Department head or delegate has accepted any unmitigated risks.

   2.3. Users must use GoA-provided accounts to access GoA on premise and Cloud resources, and for all GoA communications.

   2.4. Users must not transmit protected information/material via the internet or email that is not appropriately protected by authorised secure transfer methods or applications.

   2.5. Users must avoid accessing sites or engaging in practices that could:

   - Impact the delivery of GoA IT services;
   - Promote, display, or disseminate Offensive Materials;
   - Access illegal sites;
   - Harm the reputation of either the Alberta Public Service, the employer or the Government of Alberta,
   - Promote personal lobbying or personal advocacy groups,
   - Disseminate union materials or conduct union business, or;
   - Promote personal business activities for financial gain, or any activity considered to be a conflict of interest such as lobbying, or advocacy is strictly prohibited.

3. **Acceptable Use of GoA Content (data and information):** Maintaining the confidentiality, integrity, and availability of organizational content is paramount to the security and success of the GoA.

   The following requirements are defined to keep content secure and handled appropriately:

   3.1. Users must observe and honour all applicable intellectual property rights (i.e. copyright, patent, trademark, license agreement) governing the downloading, distribution or use of items such as text, graphics, music, or software.

   3.2. Users must protect content from theft, loss, or any unauthorized access, and must report incidents promptly to GoA Service Desk. The GoA Service desk will immediately make Cybersecurity Division aware of the incident.

   3.3. GoA content must be managed in compliance with applicable GoA policies, standards, and procedures

   3.4. GoA content must be stored on approved GoA on premise and cloud systems;

   3.5. Employees must not save GoA content classified as protected to personal cloud storage, home computers, or personal devices,

   3.6. Employees must not create, send, forward, or receive GoA content classified as Protected A, B or C using personal accounts.(If sensitive or protected information is received, employees must report the incident promptly.)

   3.7. Storage of personal content on GoA IT systems is discouraged, as all copies of data and information stored on GoA systems is the property of the Government of Alberta and subject to review for responsiveness to information access requests, investigations, and legal proceedings.

   3.8. The GoA is not responsible for the maintenance or storage of personal content and it may be deleted without notice. Employee should not expect recovery of personal content or restitution for loss of personal content.

Definitions

Confidential Information: Applies to information and data assets that, if compromised, could cause injury to the Government of Alberta. This is information that is formally classified as Protected A, B or C.

Communication and Collaboration Services: Systems provided by the Government of Alberta for exchanging information between authorized users and/or the public. Examples include Microsoft Outlook, Microsoft Teams, and GoA Videoconferencing.

GoA Content: Applies to content such as GoA Applications (Apps), digital files, data and information that are owned or licensed by the Government of Alberta.

GoA Information Technology (IT) Services: IT services provided by the GoA to facilitate government related activities. The term encompasses computer and mobile devices, Internet connectivity, communication and collaboration services, GoA applications, and GoA-related cloud services. It also includes email addresses, user accounts and social media accounts utilized by the government.

GoA Employees, Staff and Users: Persons authorized to access GoA IT Services to carry out their daily work duties, includes, but is not limited to, GoA employees, contractors, vendors and service providers, agents, contractors, volunteers, appointees, interns, and students working with a public body and organizations established by the Alberta Public Service Act.

Offensive Material: Includes, but is not limited to pornography, hate literature, obscene materials, materials which contravene human rights legislation, material used to incite violence or any other material that could reasonably be interpreted as a form of sexual or workplace harassment.

Owns/Ownership: Government of Alberta means the Crown in the Right of Alberta owns the contents of data and information stored or transmitted by equipment and systems.

Personal Content: Digital files not related to work duties, including personal documents, apps, pictures, albums, music or other content that may have been stored on GoA systems.

Personal Use: Activities not related to work duties.

Protected Information: Sensitive information that may be personal, proprietary, or Confidential in nature, the unauthorized release of which may cause physical, monetary or reputational harm to persons or entities, such as, governments or organizations.

Roles and Responsibilities

Department Heads:

1. Reserve the right to review and investigate an individual's internet or email activity where misconduct may be occurring.
2. Review allegations regarding inappropriate use of the internet or email brought to their attention by managers, system administrators, employees or others and seek guidance from the Public Service Commission for reviews.
3. Report issues to Public Service Commission who will determine next steps.

Managers:

1. Report security incidents, loss or theft of data promptly as per the applicable policy /procedure.
2. Take appropriate steps to initiate removal of access when the employee leaves the GoA or no longer performs specific work duties.
3. Ensure staff complete mandatory Cybersecurity, FOIP and IM training required for their position.
4. Ensure all staff meet their obligations to undertake precautions to safeguard data, information and systems/applications as per GoA APS guidelines for Safeguarding Government Information and follow Information Security Management Directives (ISMD) and that staff are aware of examples of security and privacy incidents and their obligation to report these in a timely manner.

GoA Employees:

1. Report security incidents, loss or theft of data promptly as per the applicable policy and procedures.
2. Do not share passwords or other information that could lead to their GoA user accounts or their access to information privileges being compromised.
3. Do not attempt unauthorized access or bypass of GoA, or any entity's, security measures or intentionally act in such a way to disrupt GoA or any other entity's network services.
4. Authorized users are not permitted to look at information about others or themselves unless there is an operational/business need to do so.
5. Do not introduce malicious code into the network or a system (e.g. viruses, worms, Trojan horses, malware, etc.)
6. Complete mandatory Cybersecurity, FOIP and IM training required for their position.
7. Undertake precautions to safeguard data, information and systems/applications as per GoA APS guidelines for Safeguarding Government Information. and fulfill obligations under Information Security Management Directives (ISMD)

Cybersecurity Division:

1. Performs investigations for activities that may violate this directive, or any law or regulation and report results to appropriate personnel.
2. Evidence of misuse may result in suspension or termination of the account or access to systems at the discretion of Cybersecurity Division. Furthermore, it may be reported to Public Service

Commission for disciplinary action up to and including dismissal, or in the case of non-employees, the termination of a contract or arrangement with the contractor, vendor, or agent.

3. Works with IMT service providers to support requirements to meet FOIP requests, legal proceedings, and internal investigations, and maintain confidentiality of these requests.

Compliance

In cases where it is determined that a breach or violation GoA policies has occurred, the Chief Information Security Officer and the respective Ministry will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Consequences of non-compliance with this policy could result in damage to Government of Alberta's reputation, expose Albertans to harm and/or incur unnecessary costs.

References and Supporting Resources

Accessing GoA IT Resources with Non-GoA-Managed Devices Standard
Code of Conduct and Ethics for the Public Service of Alberta
Communication Policy
Freedom of Information and Protection of Privacy Act
GoA Data and Information Security Classification Standard
GoA Learning Management System
Health Information Act
Identifying Official and Transitory Records Guideline
Information Security Management Directives (ISMD)
Litigation Response and Information Discovery Directive
Litigation Response and Information Discovery Guideline
Personal Information Protection Act
Public Service Act
Safeguarding Government Information
Social Media Policy
Respectful Workplace Policy

Appendix 1: Guidelines for Acceptable and Unacceptable Activities

ACCEPTABLE USE	UNACCEPTABLE USE
• To accomplish job responsibilities and to further the core businesses of the Government of Alberta.	• To intentionally interfere with the normal operation of Government of Alberta IT Services; • To download Offensive Material, protected documents, copyrighted music, images or other electronic files that may infringe on intellectual property rights
• To communicate with work-related professional contacts.	• To reveal or publicize Protected Information; • To make or post indecent, harassing, or hateful remarks about individuals or groups. • To sign up self or other GoA users for sites or services that may bring the GoA into disrepute • To impersonate other GoA users.
• To improve familiarity with the range and the depth of the information on the internet without stressing the ministry's network.	• To conduct illegal activities; • To access gambling sites, sites which support discrimination against individuals or groups protected by human rights legislation, or sites containing pornographic material.
• To pursue personal development through learning.	• To use the system for financial gain through personal business interests.
• To distribute information regarding joint union/management initiatives or other union information with prior permission.	• To use the system without permission to distribute information on union business or to undertake any other personal lobbying or personal advocacy.
• To conduct research for a program, or access internet libraries and journals.	• To access applications, websites or services, which support or promote gambling, discrimination, violence against persons, governments or business entities,
Limited personal use is acceptable on personal time provided it does not interfere with the performance of work duties, a user may:	Non acceptable personal use includes: • Access streaming sites instead of performing duties

Acceptable Use of GoA IMT Assets

ACCEPTABLE USE	UNACCEPTABLE USE
• Read the news and check the weather forecast • Confirm the bus schedules • Pay bills online • Make personal travel arrangements • Subscribe to school notifications for self or others	• Storing personal photo albums or personal media folders • Use that causes disruption of GoA IT Services • Soliciting • Posting false information or disinformation • Use GoA emails to subscribe to any sites or services that bring the GoA into disrepute