Appropriate Use of Government Information and Information Technology Policy (Appropriate Use Policy)	
Office of the Chief Information Officer **Province of British Columbia**	**Version 2.0** **Date: May 2021**

TABLE OF CONTENTS

INTRODUCTION

Purpose

This policy is meant to help government employees perform their duties in accordance with applicable laws, regulations, other corporate policies, and corporate standards and procedures related to information management (IM) and information technology (IT). This policy sets out the requirements that all employees must follow when:

- accessing and managing—i.e. creating, receiving, disclosing and disposing of — government information (particularly confidential information); and
- using government IT resources.

This policy also sets out specific IM IT requirements for supervisors.

Overview

All government employees use information and government IT resources in the course of their daily work. Therefore, every employee is responsible for managing government information, protecting confidential information (including personal information) and safeguarding government IT resources.

The Province of British Columbia expects employees to follow the Standards of Conduct for Public Service Employees, use sound and prudent judgement, and act ethically in alignment with BC Public Service Corporate Values when:

- managing government information;
- using IT resources, whether or not that use is directly related to their employment duties; and
- using social media for government business or personal reasons—for more information, please see the Social Media Guidelines.

This policy is meant to help employees and supervisors understand their IM IT obligations and must be considered in conjunction with:

- the Information Management Act (IMA), which is the Province's legislation for modern IM practices;
- the Freedom of Information and Protection of Privacy Act (FOIPPA), which governs the collection, access, use and disclosure of personal information; and
- any other corporate or ministry-specific IM IT policies, standards or procedures relevant to their positions.

The Province 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, every employee should consider opportunities to address these commitments when making decisions about using government information and IT resources.

Application

This policy applies to employees of all ministries, agencies, boards and commissions that are subject to the Core Policy and Procedures Manual (CPPM).

Authority

CPPM 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

POLICY REQUIREMENTS

1. Government Information

Employees must follow applicable legislation, policies, and standards for managing information in the course of their work. This includes managing government information in accordance with applicable information schedules approved by the Chief Records Officer under the IMA as well as following the requirements listed below. To learn more about information schedules and ministry IM responsibilities, please see the Managing Government Information Policy.

General

Employees

1.1. Employees must use government-provided accounts (e.g., email) when conducting government business.

1.2. Employees must use a secure portal when accessing information on the government network, e.g., Virtual Private Network (VPN).

1.3. Employees must save government information (e.g., documents, emails) in an appropriate system on a government network, e.g., Local Area Network (LAN), Enterprise Document and Records Manager (EDRMS), line-of-business applications such as case management systems. For more information on appropriate systems, please refer to section 1 of the Managing Government Information Policy.

1.4. Employees must only dispose of government information in accordance with an approved information schedule.

1.5. Employees must dispose of transitory information that they manage when the information is no longer of value.

1.6. Employees must not, with the intent to evade either a Freedom of Information (FOI) request or request for legal discovery:
   a. willfully alter, falsify, conceal or dispose of government information (including transitory information); or
   b. direct another person to willfully alter, falsify, conceal or dispose of government information (including transitory information).

1.7. Employees must respect intellectual property rights of the Province and third parties. For example, employees must not use, reproduce, modify or distribute intellectual property without the owner's permission.

Supervisors

1.8. When an employee starts a new job, their supervisor must ensure they are made aware of the corporate and ministry policies, standards, processes, and procedures that they must follow when accessing and managing information. This includes, but is not necessarily limited to, this policy and the Information Incident Management Policy.

1.9. Supervisors must ensure that employees are made aware when a significant change occurs respecting their access to government information or IT resources, including but not limited to:
   a. access to a new information database;
   b. an approved change in their workplace (see Flexible Workplaces & Information Security), and
   c. when a new or updated version of this policy or other IM IT policy or standard directly relevant to their work is issued.

1.10. Supervisors must ensure that employees receive IM IT training appropriate to their positions.

1.11. Supervisors must ensure that employees have the appropriate level of access to information, including confidential information, that is required to perform their duties.

1.12. Supervisors must ensure that an employee's access is promptly modified or removed when the employee no longer needs the access to perform their duties.

Confidential Information

The Province is the steward of a significant amount of confidential information, including personal information, which is managed in accordance with FOIPPA. All government employees need to do their part to protect confidential information.

1.13. Employees must actively protect confidential information, especially when handling confidential information in public places (e.g., on a bus, in an airport). This includes ensuring that information is not viewable or accessible by unauthorized persons.

1.14. Employees must secure confidential information in the workplace. This may include storing confidential paper records in locked drawers or cabinets, using strong passwords and safeguarding devices used to save or access confidential information (e.g., locking or signing out of devices when they are not in use).

1.15. When sending confidential information by mail or courier, employees must use a trackable process, such as BC Mail or external couriers. Decryption passwords must not accompany encrypted storage devices that are mailed or couriered.

1.16. Employees must limit the amount of confidential information, particularly personal information (which is subject to legal restrictions), that is circulated, including through email or other communications such as instant messages, letters, faxes, etc.

1.17. Employees must dispose of confidential information using secure methods that protect confidentiality. For example, confidential paper records must be disposed of in locked shredding bins.

1.18. Supervisors must review employees' access to confidential information annually to ensure the access remains necessary and appropriate.

1.19. If an information incident occurs, employees and supervisors must follow the Information Incident Management Policy, which requires the immediate reporting of any suspected or actual information incident (including a privacy breach or cyber-attack/phishing)

2. Government IT Resources

2.1 Employees must securely manage and protect any government IT resources in their use. For specific information on mobile device management, please refer to the Mobile Device Guidelines.

2.2 Reasonable personal use of government IT resources by employees is permitted. Personal use is reasonable provided it is lawful, in line with the Standards of Conduct and:

a. is limited during core business hours and does not interfere with the employee's duties and responsibilities;
b. does not compromise the security of government IT resources or government information, specifically confidential information; and
c. is not used for personal financial gain.

2.3 To protect personal privacy, and to reduce government's digital storage costs, employees must limit the amount of information that they store on government networks for personal reasons (e.g., family photos, personal documents).

2.4 Employees must not willfully or knowingly allow viruses (e.g., malware, phishing), spam/junk email, or other malicious content to be introduced to government IT resources, including government-issued devices and government networks.

2.5 Employees must securely manage and protect the usernames and passwords they use to access government IT resources. This includes not:

a. sharing credentials with colleagues or supervisors;
b. divulging passwords for technical support; or
c. replicating their IDIR passwords to access non-government applications (e.g., Trello, Facebook, Twitter, LinkedIn).

2.6 Employees must immediately notify the 7-7000 Service Desk (250-387-7000) if they know of or suspect potential harm or risk to the network or any government IT resources (e.g., account compromise, cyber attack, phishing).

2.7 Employees must report any lost or stolen IT resource as per CPPM Chapter 20. A lost or stolen IT resource is considered an information incident.

2.8 Employees must follow the Asset Disposal Process, as well as any relevant ministry or business-area policies and procedures, when disposing of government IT resources.

3. Applications and Software

3.1 If an employee wishes to use a government IT resource to access or download an application or software that is available via a BC Government–supplied App Store (e.g., OCIO My Service Centre, Software Center, iStore) or a ministry-specific software ordering process), the employee must obtain the applications or software from one of those sources.

3.2 If an employee wishes to use a government IT resource to access or download an application or software that is not available via a BC Government–supplied App Store or ministry-specific ordering process, the employee must first obtain their supervisor’s permission.

3.3 Supervisors must not permit an employee to download or use applications or software that:

a. are prohibited by the Office of the Chief Information Officer;
b. present unacceptable privacy or security risks;
c. impose terms and conditions, such as indemnification clauses, that are unacceptable to government (see CPPM Chapter 6).

If you have questions about specific applications or software, please contact your Ministry Information Security Officer.

4. Monitoring and Investigations

4.1 Any collection, access, use, transmission, or disposal of government information or use of government IT resources, including personal use, may be audited, inspected, monitored and/or investigated to:

a. maintain, repair and manage IT resources for the efficient operation of business systems;
b. meet legal requirements to produce information, including litigation document discovery;
c. ensure accessibility of government IT resources for the continuity of work processes;
d. improve business processes and manage productivity; and
e. ensure compliance with legislative and policy requirements, including the Standards of Conduct.

4.2 Allegations of inappropriate access, collection, use, disclosure, or disposal of government information or inappropriate use of government IT resources may be investigated. Investigations may include, but are not limited to, the search and/or seizure of IT resources.

4.3 Employees who inappropriately access, collect, use, disclose or dispose of government information or inappropriately use IT resources may be subject to disciplinary action, including dismissal, contract cancellation, and/or other legal remedies.

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 policies and procedures are developed, where necessary, to support employee compliance with, and ministry monitoring of, this policy; and
- Provide support to supervisors in their respective ministries to ensure that supervisors have the information and training necessary to fulfill their responsibilities as set out in this policy.

Supervisors

Government supervisors have the responsibility to:

- Ensure that employees are made aware of their IM IT obligations, including requirements outlined in this policy and IM IT training requirements;
- Enable employees to meet their IM IT obligations;
- Ensure that service provider contracts adequately address IM IT; and
- Ensure that employees have appropriate access to government information and IT resources to support them in carrying out their work-related duties.

Employees

All government employees have the responsibility to:

- Be aware of and fulfill their IM IT obligations, including requirements outlined in this policy;
- Actively protect confidential government information and government IT resources; and
- Seek direction from their supervisors if they have questions regarding their IM IT obligations, including requirements outlined in this policy.

DEFINITIONS

Confidential information: A category of government information (as defined under the IMA) with confidentiality requirements. Confidential information includes, but is not limited to:

- Cabinet confidences (for example, a briefing note to Cabinet);
- government economic or financial information (for example, information about a proposed administrative plan that has not yet been implemented or made public);
- information harmful to intergovernmental relations (for example, information received in confidence from another government);

- third-party business information, where its disclosure could harm the third party;
- personal information; and
- legal advice or law enforcement information.

Device: An IT resource that can connect (wired, wireless or cellular) to the government network, including but not limited to desktop computers, laptops, tablets, cellphones, smartphones, portable storage devices and access cards.

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

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called a cipher or code) to make the information unreadable to anyone other than those possessing special knowledge, usually referred to as a key.

Freedom of Information (FOI) request: An access request made under Part 2 of FOIPPA for records held by government.

Government information: As defined in Part 1 of the IMA.

Government network: A computer system in a data centre that has met the approved security requirements for the storage of confidential information (e.g., an employee's network drives). This does not include the hard drives of computers, laptops, tablets, smartphones. or other devices.

Information incident: A single or a series of events involving the collection, storage, access, use, disclosure, or disposal of government information that threaten privacy or information security and/or contravene law or policy.

IT resources: Information and communication technologies that include but are not limited to information systems, devices, streaming video, social media, and the government electronic network.

Personal information: Recorded information about an identifiable individual other than business contact information. Personal information is a type of confidential information.

Portable storage device: A portable (or removable) device that is primarily designed to store digital information (e.g., an external hard drive or a USB flash drive).

Privacy breach: The theft or loss, or the access, collection, use or disclosure of personal information that is not authorized by Part 3 of FOIPPA. A privacy breach is a type of information incident.

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.

Workplace: Any location where government business is conducted, including a traditional office facility, an employee's home, a public space or a mobile workspace.

REVISION HISTORY

Version	Date	Notes
1.0	March 21, 2014	Approved by the Government Chief Information Officer.
2.0	May 21, 2021	Approved by the Government Chief Information Officer and Chief Records Officer; revised for clarity, to align with the *Information Management Act*, and to update the definition of "workplace".
2.0	October 12, 2021 May 4, 2022 May 9, 2023	Broken links fixed