Office of the Chief Information Officer

POLICY NAME Information Security Policy V4.01	
PROGRAM AREA Information Security	EFFECTIVE DATE: 2018-09-21 LAST REVISION: 2021-11-23

Purpose and Objectives	The Information Security Policy (ISP), and the Core Policy and Procedures Manual (CPPM), specifically CPPM Chapter 12 and CPPM Chapter 15, establish the BC Government's corporate approach to information security management. The Information Security Policy acts as the framework under which all ministries must operate in order to ensure the information security practices of the Government of BC are reasonable, appropriate, and efficient. This in return will ensure the reasonable protection of personal and confidential information in a manner that is compliant with the security requirements of the *Freedom of Information and Protection of Privacy Act* and the *Information Management Act*.
Scope	This policy applies to all ministries, agencies, boards and commissions that are subject to Core Policy.

Table of Contents

Roles and Responsibilities	The **Government Chief Information Officer** and the **Chief Records Officer** share responsibility for providing corporate strategies, policies, standards and guidelines on information security. **The Office of the Chief Information Officer (OCIO)** must: (a) Maintain and review annually the Information Security Policy; and, (b) Inform Ministry Chief Information Officers of significant changes to the Information Security Policy. The **Chief Information Security Officer (CISO)** must: (a) Provide cross-government leadership for information security; (b) Manage the corporate information security risks for government; (c) Establish a program to manage and coordinate information security activities across government; (d) Monitor for, assess, and respond to, information security threats and exposures; (e) Provide evidentiary support and analysis of digital evidence in support of suspected or actual information incidents; and, (f) Assist ministries in performing information security activities. **Ministry Chief Information Officers (MCIO)** must appoint a Ministry Information Security Officer. **Ministry Information Security Officers (MISO)** must: (a) In collaboration with their Ministry Chief Information Officer and the Chief Information Security Officer, develop and maintain security controls to protect the confidentiality, integrity and availability of government information, throughout its lifecycle; (b) Manage ministry-specific information security risks; and, (c) Manage the ministry information security program. **Supervisors** must: (a) Ensure promotion of information security initiatives within their ministries; (b) Maintain awareness of government information security policies and processes; (c) Employ appropriate controls to reduce the risk of disruption of information systems such as unauthorized or unintentional modification or misuse of information systems; and, (d) Integrate information security into the organization's project management and change management processes to identify and address information security risks. ***Additional resources:*** CPPM Chapter 12: IM/IT, Privacy Breaches, Appropriate Use Policy, CPPM Chapter 15: Security.

Policy Details

1. Personnel Security

This section identifies security responsibilities and management processes throughout the employment cycle.

Supervisors must ensure:

(a) Prior to employment, employee security screening is done in accordance with Public Service Agency policies and practices;

(b) During employment, employees are informed about the information security policies and procedures, information security roles and responsibilities;

(c) At termination of employment, employees are reminded of their ongoing confidentiality responsibilities in accordance with the Standards of Conduct;

(d) Potential or actual information security breaches are investigated and reported, and invoke incident management processes where necessary; and,

(e) Contractor responsibilities for information security are identified in contractual agreements.

Additional resources: Privacy Breaches, BC Public Service Agency - Human Resource Policies, including Standards of Conduct and Oath of Employment.

2. Management of Information Systems and Devices

This section defines requirements for secure management of government information systems and devices.

Ministries must:

(a) Maintain an inventory of government information systems and devices, including portable storage devices, and mobile devices;

(b) Validate the measures taken to protect information systems and devices as part of an enterprise risk management strategy. This includes maintaining, documenting, verifying and valuing asset inventories on a regular basis;

(c) Document the return of government devices in the possession of employees upon termination of their employment;

(d) Remove government information from devices that are no longer needed by government; and,

(e) Securely dispose of devices in a manner appropriate for the sensitivity of the information the device contained.

2.1. Mobile Device Security

Ministries must ensure controls are implemented to mitigate security risks associated with the use of mobile devices.

Mobile device users must lock and/or secure unattended mobile devices to prevent unauthorized use or theft.

Additional resources: Mobile Device Security Standard, CPPM Chapter 12: IM/IT, Appropriate Use Policy, Mobile Device Guidelines.

3. Access to Information Systems and Devices

This section identifies security roles, responsibilities and management processes relating to access and authorization controls for government information systems and devices.

Ministries must define, document, implement, communicate and maintain procedures to ensure access to government information systems and devices are granted to individuals based on business requirements and the principles of "least privilege" and "need-to-know."

Supervisors must:

(a) Ensure the assignment and revocation of access rights follow a formal and documented process; and,

(b) Regularly, and upon change of employment, review, and update where appropriate, employee access rights to ensure they are accurate and up-to-date.

Employees must know and adhere to password security practices provided in the Appropriate Use Policy.

Additional resources: CPPM Chapter 12: IM/IT, Appropriate Use Policy.

4. Information Encryption

This section defines encryption methods for improving the protection of information and for reducing the likelihood of compromised sensitive information.

The Office of the Chief Information Officer must:

(a) Provide direction and leadership in the use of encryption and the provision of encryption services, including those used for user registration; and,

(b) Set corporate direction for the management (generating, storing, archiving, distributing, retiring and destroying) of encryption keys throughout their lifecycle.

The Chief Information Security Officer supports, and provides advice on the use of encryption technologies in government.

Ministries must:

(a) Select information encryption controls during system design to provide appropriate protection commensurate to the information value and security classification; and,

(b) Register the use of encryption technology products and services with the Chief Information Security Officer.

Additional resources: Cryptographic Standards.

5. Physical and Environmental Security

This section identifies operational requirements for protecting facilities where government information and information systems are located.

Ministries in collaboration with the Ministry of Citizens' Services, must:

(a) Design, document and implement security controls for a facility based on an assessment of security risks to the facility;

(b) Review, and where appropriate test, physical security and environmental control requirements;

(c) Establish appropriate entry controls to restrict access to secure areas, and to prevent unauthorized physical access to government information and devices;

(d) Incorporate physical security controls to protect against natural disasters, malicious attacks or accidents; and

(e) Ensure security controls are maintained when computer equipment, information or software is used outside government facilities.

Additional resources: Physical and Environmental Security Standard.

6. Operations Security

This section establishes a framework for identifying requirements to control, monitor, and manage information security changes to the delivery of government services.

Ministries must:

(a) Plan, document and implement change management processes to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems;

(b) Monitor and maintain information systems software throughout the software lifecycle;

(c) Define, document, assess, and test backup and recovery processes regularly;

(d) Implement processes for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems;

(e) Ensure operating procedures and responsibilities for managing information systems and information processing facilities are authorized, documented and reviewed on a regular basis;

(f) Establish controls to protect log files from unauthorized modification, access or disposal;

(g) Establish processes to identify, assess, and respond to vulnerabilities; and,

(h) Enable synchronization of computer clocks to ensure integrity of information system logs and accurate reporting.

The Chief Information Security Officer must assess, provide advice, monitor response progress, and report on vulnerability response activities.

Additional resources: Operations Security Standard

7. Computer Network and Communication Security

This section identifies requirements for the protection of sensitive or confidential information on computer networks.

The Government Chief Information Officer must provide direction and leadership on implementation of, and significant modification to, electronic messaging systems.

The Chief Information Security Officer must develop corporate security controls to protect information from interception, copying, misrouting and unauthorized disposal when being transmitted electronically.

Ministries in collaboration with the Office of the Chief Information Officer must:

(a) Document network security controls prior to commencement of service delivery;

(b) Ensure security features are implemented prior to commencement of service delivery;

(c) Document, implement and manage changes to network security controls and security management practices to protect government information systems from security threats;

(d) Ensure segregation of services, information systems, and users to support business requirements based on the principles of least privilege, management of risk and segregation of duties;

(e) Ensure implementation of network controls to prevent unauthorized access or bypassing of security control;

(f) Ensure electronic messaging services are protected commensurate to the value and sensitivity of message content, and approved for use by the Government Chief Information Officer; and,

(g) Ensure information transfers between government and external parties are protected using services approved for use by the Government Chief Information Officer.

7.1. Working remotely

This section defines information security requirements that apply to employees when working remotely.

Information security requirements that apply to employees working remotely are defined in the Telework Agreement and the Appropriate Use Policy.

Ministries must:

(a) Ensure that government information and devices are protected regardless of the type of access or physical location of employees; and,

(b) Develop and communicate policies and processes specific to areas that govern teleworking and ensure that Telework Agreements are in place.

Additional resources: Appropriate Use Policy, Flexible Work in the BC Public Service, Telework Agreement.

8. Information System Procurement, Development and Maintenance

This section defines requirements to ensure security controls are included in business and contract requirements for building and operating secure information systems, including commercial off the shelf and custom-built software.

Ministries must:

(a) Develop, implement and manage the processes and procedures necessary to ensure that information security risks and privacy requirements are taken into account throughout the systems development lifecycle;

(b) Ensure sufficient resources and funding are allocated to complete the necessary information security tasks;

(c) Ensure that system development or acquisition activities are aligned with government information security requirements and standards; and,

(d) Apply vulnerability scanning, security testing, and system acceptance processes commensurate to the value and sensitivity of the information system.

The Office of the Chief Information Officer must provide corporate direction and oversight for developing and implementing security standards to procure, develop and maintain information systems.

Additional resources: CPPM Chapter 6: Procurement, Application and Web Development and Deployment Standard, System Acquisition Development and Maintenance Security Standard.

9. Supplier Relationships

This section defines requirements to ensure supplier agreements for information systems and cloud services align with government security policies, standards and processes.

Ministries must:

(a) Ensure identified security requirements are agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities;

(b) Ensure security controls, service definitions, and delivery levels are identified and included in agreements with external parties prior to using external information and technology services;

(c) Establish processes to manage and review the information security controls of services delivered by external parties, on a regular basis;

(d) Ensure that changes to the provision of services by suppliers of information system services take into account the criticality of the information and information systems involved and the assessment of risks;

(e) Assess business requirements and associated risks related to external party access to information and information systems; and,

(f) Ensure the risks of external party access to information and information systems are identified, assessed, mitigated and managed.

9.1. Cloud Services Security

The Office of the Chief Information Officer provides corporate direction and leadership on the secure use of cloud services by:

(a) Establishing policy and providing strategic direction on the use of cloud services;

(b) Establishing roles and responsibilities; and,

(c) Establishing information security requirements for cloud services.

Ministries must:

(a) Notify the Government Chief Information Officer and the Chief Records Officer prior to procuring cloud services;

(b) Consider existing cloud service offerings provided by the Office of the Chief Information Officer prior to procuring new cloud services; and,

(c) Ensure new cloud services align with the Cloud Security Schedule provided by the Office of the Chief Information Officer.

Additional resources: Cloud Security Schedule, Security Threat and Risk Assessment (STRA) Process, Privacy Impact Assessment (PIA).

10. Information Incident Management

This section addresses the response and management of information incidents, including privacy breaches, in order to take the appropriate steps to mitigate the risk of harm.

Employees must immediately report suspected or actual information incidents in accordance with the Information Incident Management Policy.

Ministries must establish ministry specific information incident management policies and procedures, as appropriate, to ensure quick, effective and orderly response to information incidents within the ministry.

Additional resources: Privacy Breaches, Information Incident Management Policy.

11. Business Continuity Management

This section defines requirements to prepare, and re-establish, business or services as swiftly and smoothly as possible in adverse situations.

Emergency Management BC coordinates government-wide business continuity plans to reconcile recovery priorities, business impacts, security impacts and business resumption processes.

Ministries must:

(a) Establish, document, implement, and maintain processes, procedures and controls to ensure the required level of information security for business continuity and disaster recovery during an adverse situation;

(b) Ensure that vital records and critical systems are identified in business continuity plans;

(c) Review business continuity and recovery plans annually to ensure they are current, valid, functional and readily accessible during a business interruption; and,

(d) Regularly conduct business continuity and recovery exercises and, where necessary, update business continuity and recovery plans.

Additional resources: Critical Systems Standard, CPPM Chapter 16: Business Continuity Management, Emergency Management BC.

12. Assurance and Compliance

This section defines requirements to ensure compliance with legislation, government policies and standards.

The Chief Information Security Officer must:

(a) Initiate an independent review of the overall government information security program on a regular basis; and,

(b) In collaboration with ministries, report on each ministry's adherence to the information security policies, and standards.

Ministries must:

(a) Ensure the legislative, statutory, regulatory and contractual security requirements of information systems are identified, documented, addressed and maintained; and,

(b) Regularly review information systems and information security procedures to ensure compliance with security policies and standards.

Additional resources: Core Policy Procedures Manual (CPPM), Information Management Act, Standards of Conduct.

Definitions	**Availability** - Information or information systems being accessible and usable on demand to support business functions. **Business Continuity Plans** - contain the recovery procedures and strategies necessary to resume critical services and are activated when standard operational procedures and responses are overwhelmed by a disruptive event as defined in CPPM Chapter 16: Business Continuity Management. **Confidentiality** - Information is not made available or disclosed to unauthorized individuals, entities or processes. **Control** - any policies, processes, practices or other actions that may be used to modify or manage information security risk. **Cryptography** - the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use. **Device** - An IT Resource that can connect (wired, wireless or cellular) to the government network, including but not limited to computers, laptops, tablets, smartphones, and cellphones. **Employee** - an individual working for the Government of British Columbia, including Service Providers or volunteers. **Government Network** - the equipment, information systems and cabling systems used to establish a government communication network between Information Systems. **Information processing facilities** - the physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal. **Information Incident** - is a single or a series of unwanted or unexpected events that threaten privacy or information security. **Information System** - A system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output and control functions in relation to information and data. Normally used to describe computerized systems, including data processing facilities, data base administration, hardware and software which contain machine-readable records. A collection of manual and automated components that manages a specific data set or information resource as defined in CPPM Chapter 12: IM/IT. **IT Resources** - information and communication technologies that include, but are not limited to, information systems, devices and the government electronic network. **Integrity** - the characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated or unintentional modification.

	Least Privilege - a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use. **Mobile Devices** - Portable self-contained electronic devices, including laptops, tablets, smartphones, cell phones, digital cameras, etc. **Need-to-know** - a principle where access is restricted to authorized Employees that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office. **Security Screening** - verification of facts about individuals related to their identity, professional credentials, previous employment, education and skills. **Telework** - Work done away from the office, also known as telecommuting. Most telework is work from home as defined in Flexible workplaces. **Threat** - potential cause of an unwanted incident, which may result in harm to a system or organization. **Vulnerability** - weakness of an asset or control that can be exploited by one or more threats.
Authority	Core Policy and Procedures Manual
Monitoring	The OCIO will review this policy annually, including consultation with stakeholders, and will make updates as required.
Related Information	FOIPPA Policy & Procedures Manual Information Management Act Core Policy Procedures Manual (CPPM) • CPPM Chapter 6: Procurement • CPPM Chapter 8: Asset Management • CPPM Chapter 12: IM/IT • CPPM Chapter 15: Security • CPPM Chapter 16: Business Continuity Management Information Management / Information Technology Standards (IM/IT Standards) Privacy Breaches Appropriate Use Policy BC Public Service Agency - Human Resource Policies, including Standards of Conduct and Oath of Employment Cloud Security Schedule

General Services Agreement (GSA)

Security Threat and Risk Assessment Process (STRA Process)

Privacy Impact Assessment (PIA)

Inquiries	Inquiries and update/change notifications about this policy can be directed to Information Security Branch, OCIO at: CITZCIOSecurity@gov.bc.ca.

Revision History

Version	Revision Date	Author	Description of Revision
4.0	2018-09-19	Clive Brown	Complete rewrite of ISP V3.0
4.01	2021-11-23	Kristina Petrosyan/Sarah Browning	Minor edits, links update.