Government of Alberta

Information Security Management Directives (ISMD)

Version 2.4

January 16, 2023

Prepared by:
Cybersecurity Division

Table of Contents

Version History

Date	Author	Version	Change Description
January 2, 2012	Tim McCreight	1.0	Initial/original 10 documents outlining the 10 information security management directives.
February 27, 2017	Martin Dinel	2.0	Consolidated version of the ISMDs in one document.
May 30, 2019	Kenneth Lummis	2.1	2019 ISMD Review – realign to NIST
December 5, 2019	Martin Dinel	2.2	Address comments from review and few typos
January 29, 2020	Martin Dinel	2.3	Incorporated feedback from AMD IMT, 2020-01- 28 meeting
February 7, 2020	Martin Dinel	2.3	Minor: formatting and grammatical changes
February 20, 2020	Martin Dinel	2.3	Minor: Removed 2 duplicate controls
Oct 14, 2022	Martin Dinel	2.4	Governance update to align with reorg of CS Division.
December 20	Gity Rabiee	2.4	Updated based on feedback received from Health, Treasury Board and Finance and IMT policy team
May 3, 2023	Gity Rabiee	2.4	Removed the Authority section

Purpose

The Information Security Management Directives establish corporate security requirements for Information Management and Technology (IMT) systems, and organizational roles and responsibilities for information security management within the Government of Alberta (GoA) and its departments.

The directive statements identify the controls necessary to implement foundational IMT security within the Government of Alberta. GoA security standards and other policy instruments provide further information regarding the details surrounding the implementation of these directives.

GoA policy instruments, standards, the cybersecurity framework, controls, processes, and procedures, support these directives.

The foundation for the controls is NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations.

Scope

These directives apply to all GoA departments except for Health, IMT systems, the information processed or stored by those systems, and all users of those systems. These directives are applicable to all IMT systems and Data, whether hosted in house or off premise, including cloud-based services and solutions.

It is important to note that some departments may have additional security directives and controls due to requirements specific to the data collections under their accountability and responsibility. For example, the Ministry of Health has additional and specific directives due to requirements outlined in the *Personal Information Protection and Electronic Documents Act (PIPEDA) and the Health Information Act (HIA).* These directives complement, or in case of conflicts, take precedence over the ISMDs when applied to information and data assets under these departments' accountability and responsibility.

Directive Statements

1. Identify

1.1 Governance

1.1.1 The Deputy Minister of Technology and Innovation is accountable for the overall provision of the Cybersecurity Program implemented across the GoA and its departments.

1.1.2 The Assistant Deputy Minister (ADM) of the Cybersecurity Division and Chief Information Security Officer is accountable to the Deputy Minister of Technology and Innovation and has overall responsibility for delivering corporate cybersecurity services.

1.1.3 The ADM of the Cybersecurity Division is accountable for the development and implementation of Information Security controls, standards, and processes implemented across the GoA and its departments.

1.1.4 The ADM of the Cybersecurity Division is accountable for monitoring and reporting security controls compliance across the Government of Alberta.

1.1.5 The ADM of the Cybersecurity Division is accountable for monitoring and reporting security incidents across the Government of Alberta.

1.1.6 The ADM Cybersecurity Division is responsible for facilitating the implementation of Information Security controls, standards, and processes across the GoA and its departments, to monitor compliance to security controls, standards, and processes, and to report non-compliance or compliance issues to department heads, including to the Deputy Minister of Technology and Innovation.

1.1.7 The ADM of the Cybersecurity Division is responsible for monitoring and reporting security and privacy risks relating to information and technology assets across the GoA; and providing advice and recommendations to departments regarding these risks, treatment plans, and security controls.

1.1.8 Department heads are accountable for compliance with Information Security Management Directives, controls, standards and practices for data collections and systems under their stewardship.

1.1.9 Department heads are accountable for reporting compliance results to the ADM of the Cybersecurity Division.

1.1.10 Department heads are accountable for the security of the information collected, created, or maintained by their department. They retain the role of Information Controller for all data collections under their stewardship, unless the role is explicitly assigned to a report within the department.

1.1.11 Department heads are responsible for assigning Information Controllers to Information Assets and IMT systems.

1.1.12 Digital Design and Delivery (3D), Technology Support and Operations (TSO)

and Cybersecurity Division are responsible to department heads for delivery of secure solutions.

1.1.13 Cybersecurity Division Service Managers provide advice and consultation to the GoA for cybersecurity policy instruments, controls, and risks across the GoA.

1.1.14 Information Controllers ensure the security requirements for their Information Assets and IMT systems are met.

1.1.15 Department heads or their delegates are responsible for accepting risks and treatment plans for their systems. Risk cannot be ignored.

1.1.16 Information Custodians are responsible for implementing security controls to satisfy identified security requirements for Information and Information Technology Systems.

1.1.17 Security roles, clearance requirements, and responsibilities must be clearly defined for all information and IMT systems.

1.2 Asset Management

1.2.1 All departments must document, classify, and maintain an inventory of their information assets and IMT systems in Configuration Management Database (CMDB).

1.2.2 Information must be classified and managed in accordance with GoA Information Management standards.

1.2.3 Users of information and IMT systems must take responsibility for and accept the duty to actively protect GoA information and technology assets.

1.2.4 Non-disclosure agreements (NDA) for protecting information must be established and reviewed regularly.

1.2.5 Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information between organizational entities through all types of communication services.

1.2.6 Information exchange agreements between the GoA and other external organizations must be documented.

1.2.7 Security requirements must be identified and addressed prior to granting external parties access to GoA information or IMT systems and established through contract.

1.2.8 Personnel must return all GoA assets upon termination or change of employment.

1.3 Business Environment

1.3.1 All procurement must be conducted in accordance with the GoA's Procurement Accountability Framework (PAF) for all IMT systems acquisitions, contracts,

developments, services, and upgrades.

1.3.2 Equipment must be protected from unauthorized access, environmental threats and hazards, and disruptions.

1.4 Risk Assessment

1.4.1 Risk assessments, including the documentation of risk treatment plans, must be performed for all Information Assets and IMT systems in advanced of implementation. Identified risks and mitigation plans to be entered in the Corporate IMT Risk Register.

1.4.2 Information sensitivity, regulatory requirements, systems criticality, and security or clearance requirements must be identified as part of business requirements.

1.4.3 Access to IMT systems and services must be consistent with business needs and based on asset's information security classification, risk, and security assessments.

1.4.4 Security controls must be implemented to mitigate risks associated with the interconnection of business IMT systems.

1.5 Risk Management

1.5.1 Security requirements must be documented, approved, and integrated into the management of IMT systems throughout its lifecycle.

1.5.2 Security designs, for implementations and updates of IMT systems, must be subjected to a security review facilitated by Cybersecurity Division to ensure that potential risks are identified, assessed, and mitigated, as well as put through an appropriate approval process.

1.5.3 The security design of all IMT systems must be documented, reviewed by Cybersecurity Division, approved by the Information Controller, and implemented as specified.

1.5.4 Risks assessments must be conducted for all new IMT systems and for substantial updates to existing systems.

1.6 Supply Chain Risk Management

1.6.1 Electronic commerce IMT systems, subject to the Payment Card Industry Data Security Standard (PCI DSS), must be protected from fraudulent activity, identity theft, identity fraud, unauthorized disclosure, unauthorized access, and modification.

1.6.2 GoA security requirements must be communicated with external parties prior to commencement of service delivery agreement.

1.6.3 External parties must adhere to GoA Policy, security directives and standards established for GoA information and IMT systems. Those requirements must be established through contract.

2 Protect

2.1 Identity Management, Authentication and Access Control

2.1.1 Formal user registration and de-registration processes must be in place for granting access to all IMT systems as defined by business requirements.

2.1.2 The allocation and use of elevated privilege and special accounts must be restricted and controlled.

2.1.3 All users must be issued a unique identifier for their use only, and an approved secure authentication technique must be used to substantiate the identity of each user.

2.1.4 Authentication mechanisms must comply with approved corporate access control standards and include secure user credentials management system.

2.1.5 Operating systems and Business Systems sessions must be terminated or require re-authentication after a pre-defined period of inactivity.

2.1.6 The provisioning and de-provisioning of authentication credentials must be controlled through a formal management process.

2.1.7 Information Controllers must formally review user access rights at least quarterly and ensure access changes are documented.

2.1.8 Users must protect all authentication credentials issued to them from unauthorized use.

2.1.9 Users and systems must be provided access only to the Information and IMT systems they have been authorized to use.

2.1.10 Secure areas must be isolated from other operational zones and offices to prevent unauthorized access to sensitive information and technology.

2.1.11 Access to secure areas must be controlled, authorized, and protected by security controls.

2.1.12 Physical security zones must be defined, and controls documented and communicated to authorized personnel.

2.1.13 Physical and logical access to network devices must be securely controlled, logged, and monitored.

2.1.14 Remote access must employ security measures to protect GoA networks, servers, applications, and data.

2.1.15 Remote access to internal GoA systems must use strong authentication and comply with approved GoA authentication standards.

2.1.16 Access permissions and authorizations must be managed and incorporate the principles of least privilege and separation of duties to reduce opportunities for unauthorized modification or misuse of IMT systems.

2.1.17 A range of detective and protective technologies must be implemented to safeguard information and IMT systems within the government network.

2.1.18 Applications, users, and IMT systems must be segregated on networks (or network domains) where supported by risk assessments at the discretion of the Information Controller.

2.2 Awareness and Training

2.2.1 Employees, contractors, and volunteers must be provided with orientation on the Acceptable Use of GoA IT Assets Directive.

2.2.2 All new and existing GoA employees must complete mandatory cybersecurity awareness training annually.

2.2.3 Cybersecurity Division informs personnel of mandatory information security training and changes to information security management policy instruments.

2.2.4 New implemented security controls will be supplemented with appropriate training, exercises, and user awareness materials where these apply.

2.3 Data Security

2.3.1 All devices must be correctly maintained to enable continued confidentiality, integrity, and availability of information.

2.3.2 Media must be managed with appropriate controls for the sensitivity of the data contained on the media.

2.3.3 Where Production data is used outside of Production environments (Development, testing etc.), it must be protected with the same security controls mandated and applied to the production environment.

2.3.4 All GoA information and data in use, in transit and at rest must be appropriately protected.

2.3.5 The use of cryptographic controls must be based on the security classification of the information or system that is to be protected and must follow approved GoA encryption standards.

2.3.6 The decommissioning of information assets must comply with GoA standards.

2.3.7 Equipment content (storage devices and memory) must be sanitized prior to reassignment, disposal, destruction, or decommissioning in accordance with "Secure Media Sanitization Standard" established by Cybersecurity Division.

2.3.8 Storage media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.

2.3.9 Storage media being transported must be appropriately protected against unauthorized access, use, or modification.

2.3.10 Production and non-Production environments are to be separated where required and supported by a risk assessment.

2.4 Information Protection Processes and Procedures

2.4.1 Operating procedures and responsibilities must be documented, authorized, and maintained.

2.4.2 Security acceptance criteria for new IMT systems, upgrades and new versions must be established and carried out for new and existing solutions.

2.4.3 Security acceptance testing of the systems must be carried out prior to acceptance by the risk owner.

2.4.4 Upgrades and updates to software must include removal of previous versions.

2.4.5 Software development must be in compliance with approved GoA security standards.

2.4.6 Changes to applications and IMT systems must be controlled using formal change control processes. Change control process must include assurances that the security design and requirements are not compromised.

2.4.7 Change management processes for IMT systems services delivered by external parties must consider the criticality of the information, IMT systems, processes involved, and assessment of risks.

2.4.8 Software installation on GoA managed devices must follow an approved and documented process.

2.4.9 Information and IMT systems must be backed up and the recovery process tested regularly.

2.4.10 The departments work collaboratively with Cybersecurity Division to regularly audit IMT systems for compliance with GoA Information Security policy instruments, applicable legislation, and business requirements, and will report findings to the departments and the GoA's executive management.

2.4.11 Controls must be documented, implemented, and communicated by Control Owner or their designate to ensure compliance with applicable legal, regulatory, and contractual restrictions.

2.4.12 Processes and controls for the acceptable use of IMT systems must be identified, documented, communicated, and implemented.

2.4.13 Personnel screening must be performed prior to entering a working relationship with the GoA to an appropriate level that considers information security risks and required security clearance.

2.4.14 Managers must advise personnel to maintain confidentiality of sensitive information after termination or change of employment.

2.4.15 The access rights of personnel to IMT systems must be removed upon termination of employment and reviewed upon change of employment.

2.5 Protective Maintenance

2.5.1 Audit requirements and activities involving checks on operational systems must be planned and approved in collaboration with the Information Controllers to minimize disruption to business processes.

2.5.2 Use of system audit tools must be planned and controlled to prevent misuse or compromise.

2.6 Protective Technology

2.6.1 Data Processing Facilities must be designed with physical security perimeters that protect against natural and human induced damages and disasters.

2.6.2 Data Processing Facilities must be protected by appropriate access controls based on the security classification of the data stored within the facilities to ensure that only authorized personnel are allowed access.

2.6.3 Data Processing Facilities must be protected by environmental and emergency controls and from disruptions caused by failures in supporting utilities in a manner that satisfies hosted IMT systems' disaster recovery requirements.

2.6.4 Power and telecommunications cabling carrying data or supporting information services must be protected against interception, interference, and damage.

2.6.5 Equipment containing information or software must not be moved offsite without prior authorization. When offsite, equipment must be protected using appropriate security controls.

2.6.6 Security features, service levels and management requirements of all network services must be documented and included in all network service agreements provided in-house or outsourced.

2.6.7 Audit logs recording user activities, exceptions, faults, and information security events must be produced, protected, and monitored. Results of the monitoring activities must be regularly reviewed.

2.6.8 IMT system logging facilities and log information must be protected against tampering and unauthorized access.

2.6.9 Activities of operators and administrators must be logged, protected, monitored, and regularly reviewed.

2.6.10 Cybersecurity requirements and appropriate measures are applied in a risk-based, lifecycle approach to protect IMT services.

2.6.11 Periodic reviews of protection processes must occur and be evaluated for opportunities of continuous improvement in alignment with an established system development lifecycle.

2.6.12 Access to advice, guidance and services, and other applicable protection effectiveness will be shared as needed for informed decision-making related to government security priorities.

3 Detect

3.1 Anomalies and Events

3.1.1 Users of information and IMT systems must report cybersecurity events and incidents to Cybersecurity Division.

3.1.2 Detection, prevention, and recovery controls must be implemented according to approved GoA standards to protect IMT systems.

3.1.3 Processes and tools are to be deployed as appropriate and as defined in GoA IMT standards to detect anomalies and events.

3.2 Continuous Security Monitoring

3.2.1 Information Custodians, System and Network Administrators will regularly provide reports to Information Controllers and Service Owners on the health and status of their assigned IT assets. All GoA-IT assets must be continuously monitored.

3.2.2 Security incidents, breaches, or policy violations caused by personnel must be reported to Cybersecurity Division and reviewed by Management.

3.2.3 Security information and event management processes must coordinate, manage, and monitor vulnerabilities and threats within GoA.

3.3 Detection Processes

3.3.1 Regular risk assessments must be conducted to evaluate IMT systems.

3.3.2 Vulnerabilities, threats, and risks must be assessed, managed, and reported**.**

3.3.3 Reports of anomalies and events must be reviewed for process improvement.

3.3.4 Computer clocks must be synchronized to an approved GoA time source.

4 Respond

4.1 Response Planning

4.1.1 Security incident response processes must be developed and maintained for all information and technology assets.

4.1.2. A written agreement that defines appropriate communication and respective security responsibilities of third-party groups during an incident response must be in place.

4.2 Response Communications

4.2.1 Development and maintenance teams will work collaboratively with Cybersecurity Division to ensure that communications plans are established to notify stakeholders in the event of cybersecurity incidents.

4.2.2 The Cybersecurity Division is responsible for developing, maintaining, and communicating these plans.

4.3 Response Analysis

4.3.1 The Cybersecurity Incident Response team must determine the impact and criticality of information security incidents based on operational processes.

4.4 Response Mitigation

4.4.1 Remediation activities need to be performed and risks documented during an incident to minimize business disruption.

4.5 Response Improvements

4.5.1 Post-security incident reviews must be conducted to assess and improve the standard GoA Incident Response Plan and to mitigate future information security incidents.

5 Recover

5.1 Recovery Planning

5.1.1 The Cybersecurity Division must provide oversight, advice, and facilitation to the IT disaster recovery planning community.

5.1.2 The Cybersecurity Division is responsible to develop, maintain, and communicate the IT Disaster Recovery Framework, which includes policy instruments, standards, processes, and templates focusing on the recovery of information and systems across the GoA based on their criticality.

5.1.3 Department heads must identify IT Disaster Recovery Executive Sponsors for their department's information assets and IMT systems.

5.1.4 A managed IT Disaster Recovery Plan must be developed, coordinated, implemented, and regularly tested for all systems owned by a department.

5.1.5 Disaster Recovery plans (DRPs) must be created within the scope of the department's Business Continuity Plan (BCP) and in accordance with the Emergency Management Act.

5.1.6 The criticality of each system owned by a department must be assessed by the Information Controller and documented according to the GoA IT Disaster Recovery framework maintained by the Cybersecurity Division.

5.1.7 Information Controllers must work in collaboration with Information Custodians to ensure that identified availability and resiliency requirements for their systems can be implemented, maintained, and supported by Information Custodians.

5.2 Recovery Improvements

5.2.1 A managed IT Disaster Recovery Plan must be regularly maintained, tested, reviewed, and revised for all systems owned by a department.

5.2.2 Critical systems IT Disaster Recovery Plans must be tested, reviewed, and revised annually.

5.3 Recovery Communication

5.3.1 The Cybersecurity Division is responsible for developing, maintaining, and communicating the IT Disaster Recovery Communications plan that ensures that executives and operational teams receive appropriate communications.

Replaces Existing Policy Instruments

GoA Information Security Management Directives v2.3

Glossary of Terms

Application – a collection of computer programs, databases, and procedures designed to help the GoA perform particular tasks or handle particular types of IT problems by automating a business process or function. Also known as a business application.

Assets – for the purposes of information security policy: information in all forms and media, networks, hardware, software, and application systems.

Audit – an examination of the facts to render an opinion and would include testing evidence to support the opinion.

Audit logs – includes all types of event logs including (but not limited to) security, audit, application, access, and network across all operating system platforms.

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Strong Authentication is a method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors to authenticate (something you know, something you are, or something you have).

Availability – the property of being accessible and usable upon demand by an authorized entity.

Business Continuity Plan (BCP) – the procedures and information necessary for the timely recovery of essential services, programs, and operations, within a predefined timeframe. The BCP includes the recovery following an emergency or a disaster that interrupts an operation or affects service or program delivery.

Change management – the objective of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to minimize the impact of change-related incidents and to improve day-to-day operations.

Confidentiality – the property of information not being made available or disclosed to unauthorized individuals, entities, or processes.

Corporate Information Security Program – see **Information Security Program**.

Corporate – Government of Alberta, cross departments.

Data – see **Information**.

Data processing facility – the physical location housing any information processing system, service, or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

Department– A department supports its Minister and the government by providing advice on policies and legislation, and by implementing ministerial decisions and programs. Headed by a Deputy Minister, a department carries out activities that require regular ministerial oversight and direction**.**

Devices – Hardware that information is written to and/or stored on. See also **Hardware**.

Disaster Recovery Plans (DRP) – the procedures and information necessary to recover critical IT functions from any event that may interrupt an operation or affect service or program delivery, within the timeframes determined in the Business Impact Assessment. The DRP is part of a department's overall Business Continuity Plan (BCP).

Decommissioning – the actions taken regarding information that is no longer needed to support on-going administrative and operational activities in accordance with an approved Records Management Schedule. Directions may include destroying, transferring to the government archives, transferring to inactive records storage space, or retaining permanently in unit.

Electronic commerce – the exchange of information between government and internal and external stakeholders independently of either participant's computer system. E.g., electronically accessing forms, obtaining payments, sending invoices, receiving tax returns, placing orders, and receiving transaction acknowledgements.

Employee – is a person appointed under the Public Service Act.

Equipment – see **Hardware**.

Event – Occurrence or change of a particular set of circumstances.

Hardware – includes (but is not limited to) servers, desktop computers, printers, scanners, fax machines, photocopiers, multi-function devices, portable computing devices, routers, communications and mobile equipment, smart phones, PDAs, and removable media.

Incident - An event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (NIST).

Information - information in all forms, in any medium, and at all stages of its lifecycle, including the description of information contents; origins, structure and relationships enabling correct interpretation of information; and technologies currently in use and future technologies.

Information asset – all recorded information, regardless of physical format, that is received, created, deposited, or held by or in any department, agency, board, commission, Crown corporation, institution, committee, or council reporting or responsible to the GoA. Government records include machine-readable records; data stored in information systems; all media formats, etc.; and cabinet ministers' records that are created and/or accumulated and used by a Minister (or a Minster's office) in developing, implementing and/or administering programs of government. Government records do not include legislative records (records created and/or accumulated and used by an individual or an office in the administration of the Legislative Assembly of Alberta or by a Member of the Legislative Assembly).

Information Controllers – have the responsibility and decision-making authority for

assigned collections of information, including (but not limited to) regulating and administering the use, disclosure, and/or disposition of information. Within the Government of Alberta, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent).

Information controllership may be further delegated by the Deputy Minister.

Information Custodians – have the responsibility for maintaining and/or administering the systems and/or applications in which information is managed without having responsibility for the information itself.

Information management - involves the planning, directing, and controlling of all the government's information assets to meet corporate goals and deliver programs and services. Information management refers to the application of consistent practices related to planning, creation, capture or collection, organization, use, accessibility, dissemination, storage, protection, and disposition (either destruction or permanent retention) of information.

Information owners – Actual correct term is **Information Controllers** (see above for definition).

Information security – the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed, and improved, where necessary, to ensure that the specific security and business objectives of the Government are met. This should be done in conjunction with other business management processes. [ISO 27002].

Information security incident – is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (ISO/IEC TR 18044:2004) Information security incidents may include but are not limited to:

- Inappropriate use of government resources causing a service disruption;
- Breaches of privacy and/or confidentiality;
- Denial of service;
- Detection of network probing;
- Detection of malicious code, e.g., virus, worm or Trojan horse;
- Errors due to incomplete or inaccurate data;
- Outgoing network traffic not associated with typical business processing;
- Repeated attempts of unauthorized access;
- Repeated attempts to e-mail unknown internal accounts;
- System activity not related to typical business processing; and,
- System failures and loss of service.

Information security program - provides the security infrastructure necessary to protect government information assets by:

- Establishing an information security architecture for standard security controls across

government;
- Defining organizational roles and responsibilities for information security;
- Developing and reviewing the Information Security Policy;
- Monitoring and measuring the implementation of the Information Security Policy; and
- Developing and delivering a program to maintain information security awareness.

Information system – see: **Information technology system.**

Information technology system – any equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

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.

Malicious code – malicious code (malware) is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources. Types of malicious code can include viruses, worms, Trojans, spyware, and denial of service attacks.

Media – see: **Records**.

Monitoring – a regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards.

Multi-factor authentication – this is combining two or more authentication techniques to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: Secret - something the person knows; Token - something the person has; and Biometric - something the person is.

Operating procedure - tools which implement business processes compliant with policy, directives, and standards. Procedures are specific steps that instruct how to complete a specific task or accomplish specific objectives.

Operations – refers to all Government of Alberta production environments, both public and internal facing.

Personnel – includes employees and other individuals (e.g., contractors, consultants, volunteers, third-party organizations).

Policy - a policy is set by a Minister or by Cabinet and states what the government's position is on an issue of importance and what behaviours, or actions are expected. A policy defines a course of action, set of principles, or plans that guide, directs, or influences decision making. IMT Policies are set by the Minister of Technology and Innovation to formally state the

government's expectations for IMT and impose specific accountabilities on ministries.

Portable computing devices – portable self-contained electronic devices, including portable computers (e.g., laptops), personal digital assistants (PDAs), cell phones, digital cameras, etc.

Privacy – the right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in documents.

Record – means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other information that is written, photographed, recorded, or stored in any manner, but does not include software or any mechanism that produces records. (*The Freedom of Information and Protection of Privacy Act (FOIP Act)*.

Remote access – the act of using a remote access service to connect to the government network or government systems.

Risk – potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

Risk assessment – overall process of risk analysis and risk evaluation.

Screening – to verify facts about individuals related to their identity, professional credentials, previous employment, education, and skills.

Secure area – a site or location (such as an office or data processing facility) where physical access is restricted to authorized personnel.

Security review – an independent review with the scope focused on the security framework over the business processes, application, and operating environment. Reviews are distinguishable from audits in that the scope of a review is less than that of an audit and therefore the level of assurance provided is lower.

Security Threat and Risk Assessment (STRA) – a component of a risk analysis specifically aimed at identifying security exposures.

Service agreement – the contract or agreement between a service provider and a service consumer which defines the services to be delivered and the terms and conditions of delivery.

Software – includes (but is not limited to) application and system software, development tools, and utilities.

Standard – a set of mandatory operations or technical measures, or procedures approved for government-wide use.

System– a collection of computer hardware, computer programs, databases, procedures, and knowledge workers that work together to perform a related group of services or business processes.

Third party – includes external parties and persons outside the direct reporting structure of the Information Controller or Information Custodian (e.g., an individual, a business

or organization, personnel from another branch of government, or another level of government) Third party also include vendors, service delivery agents, businesses, and citizens.

Threat – in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental, or of natural origin. (See: **Vulnerability** and **Event**).

User – all persons authorized to access the government information or information technology systems including employees and contractors.

Vulnerability – in the security context, a weakness in security procedures, processes, or controls that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.