Government of Alberta

Information Security Management Directives (ISMD)

Version 2.3

February 20, 2020

Prepared by:

Corporate Information Security Office
Office of the Corporate Chief Information Officer and Telecommunications
Service Alberta

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

Table of Contents

Purpose

The directives stated in this document establish the corporate security requirements of Information Management and Technology (IMT) systems, and the organizational roles and responsibilities for information security management within the Government of Alberta (GoA) and its Departments. These directives are applicable to all IT Systems and Data, whether hosted in house or off premise, including cloud-based services and solutions. The foundation for the controls is NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations.

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. Directive statements are supported and elaborated using standards, operational procedures, templates, and other Policy Instruments that are all part of the GoA Cybersecurity Framework.

Scope

These directives apply to all GoA departments IT systems, information processed or stored by those systems, and all users of those systems.

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 Service Alberta is accountable for Information Security controls, standards, and processes implemented across the GoA and its Departments.

1.1.2 The Deputy Minister of Service Alberta is accountable for monitoring and reporting security compliance across the Government of Alberta.

1.1.3 The Deputy Minister of Service Alberta is accountable for monitoring and reporting security incidents across the Government of Alberta.

1.1.4 The Corporate Chief Information Officer is accountable to the Deputy Minister of Service Alberta for delivering Corporate information technology security services.

1.1.5 The Chief Information Security Officer is responsible for facilitating the implementation of Information Security controls, standards, and processes across the GoA and its department, 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 Service Alberta and to the Corporate Chief Information Officer.

1.1.6 The Chief Information Security Officer 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.

1.1.7 Department Heads are accountable for compliance with Information Security Management Directives and Standards and Practices regarding Data Collections and systems under their stewardship.

1.1.8 Department Heads are accountable for reporting compliance results to the Corporate Chief Information Officer (CCIO) through their assigned Sector Chief Information Officer (SCIO).

1.1.9 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 was explicitly assigned to a report within the Department.

1.1.10 Department Heads are responsible for assigning Information Controllers to Information Assets and IT Systems.

1.1.11 Sector Chief Information Officers (Sector CIO) assigned to a particular portfolio of departments are responsible to the Department Heads within their Sector for delivering secure solutions.

1.1.12 Sector Information Security Officers (Sector ISO) provide advice and consultation to the Sector CIOs for security controls, requirements, and risks across the Sector.

1.1.13 Information Controllers are responsible for determining security requirements for their Information Assets and Information Technology Systems.

1.1.14 Information Controllers are responsible for accepting risks and treatment plans for their systems.

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

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

1.2 Asset Management

1.2.1 All Departments must document, classify and maintain an inventory of their information assets and IT systems.

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

1.2.3 Users of information and IT systems must take responsibility for and accept the duty to actively protect GoA information and technology assets. Mandatory annual Information Security and Information Management online training is available to identify and define these responsibilities.

1.2.4 Confidentiality agreements 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 IT systems and established through contract.

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

1.3 Business Environment

1.3.1 All procurement must be conducted in accordance with the GoA's Procurement Accountability Framework (PAF) for all IT 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 IT Systems. Identified risks should 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 IT systems and services must be consistent with business needs and based on security requirements. Additional security requirements are determined by risks assessments and by the asset's information security classification.

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

1.5 Risk Management Strategy

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

1.5.2 Security designs, for implementations and updates of IT systems, must be subjected to a security review facilitated by the CISO 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 IT Systems must be documented, reviewed by CISO, approved by the Information Controller, and implemented as specified.

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

1.6 Supply Chain Risk Management

1.6.1 Electronic commerce IT systems must be protected from fraudulent activity, contract dispute, 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 security directives and standards established for GoA information and IT 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 IT 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 authentication technique must be used to substantiate the identity of each user.

2.1.4 Authentication mechanisms must comply with approved corporate standards.

2.1.5 The issuance of authentication credentials must be controlled through a formal management process.

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

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

2.1.8 Users and systems must be provided access only to the IT systems they have been authorized to use.

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

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

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

2.1.12 Physical and logical access to network devices must be securely controlled and monitored.

2.1.13 Remote access technologies must employ security controls to ensure that information resources are not compromised.

2.1.14 Remote access to internal GoA systems must require multi-factor authentication.

2.1.15 Duties and areas of responsibility are to be segregated where required to reduce opportunities for unauthorized modification or misuse of IT systems.

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

2.1.17 Applications, users, and IT systems must be segregated on networks (or network domains) where supported by risk assessments at the discretion of the information controller.

2.1.18 Access to GoA IT systems require a secure logon process.

2.1.19 A user credentials management system must be in place.

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

2.2 Awareness and Training

2.2.1 Employees, contractors and volunteers must be provided with orientation on the GoA's expectations of staff regarding information security.

2.2.2 Management must make personnel aware of mandatory information security management policy instruments.

2.2.3 Personnel must receive regular information security training and be informed of changes to information security management policy instruments and practices that apply to them.

2.2.4 Security controls implemented must be supplemented by appropriate training, exercises, and user awareness materials.

2.3 Data Security

2.3.1 Equipment 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 Information transmitted by electronic messaging must be appropriately protected.

2.3.5 The use of cryptographic controls must be based on the risk of unauthorized access and 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 Personnel must return all GoA Department assets upon termination or change of employment.

2.3.8 Equipment must be sanitized prior to reassignment, disposal, destruction, or decommissioning in accordance with procedures established by Records Management.

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

2.3.10 Media being transported must be appropriately protected against unauthorized access, use, or modification.

2.3.11 Appropriate controls must be implemented to mitigate security risks associated with the use of portable computing devices.

2.3.12 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 IT systems, upgrades and new versions must be established.

2.4.3 Security acceptance testing of the system must be carried out prior to acceptance.

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 IT systems must be controlled by the use of formal change control processes. Change control procedures must include assurances that the security design and requirements are not compromised.

2.4.7 Change management processes for IT systems services delivered by external parties must take into account the criticality of the information, IT 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 IT systems must be backed up and the recovery process tested regularly.

2.4.10 The CISO works collaboratively with Sector ISOs to regularly audit IT 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 Information Controllers or their designate to ensure compliance with applicable legal, regulatory and contractual restrictions.

2.4.12 Processes and controls for the acceptable use of IT 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 which 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 IT 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 IT 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 IT 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.

3 Detect

3.1 Anomalies and Events

3.1.1 Users of information and IT systems are responsible for reporting IT security events and incidents.

3.2 Security Continuous Monitoring

3.2.1 Detection, prevention and recovery controls must be implemented to protect IT systems against malicious code (malware) and intrusions.

3.2.2 Processes and tools are to be deployed to detect anomalies and events

3.2.3 Information Controllers must regularly monitor and review services, reports and records provided by external parties.

3.2.4 Only GoA managed devices shall be connected to internal GoA networks and connected devices must be continuously monitored.

3.2.5 Security incidents, breaches or policy violations caused by personnel must be reported to the CISO and reviewed by Management.

3.3 Detection Processes

3.3.1 Regular assessments must be conducted to evaluate IT systems. Vulnerabilities and risks must be assessed, reported and managed.

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

4 Respond

4.1 Response Planning

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

4.2 Response Communications

4.2.1 Communications are to be sent out during an incident to notify stakeholders.

4.3 Response Analysis

4.3.1 Security incident management must determine the criticality of information security incidents based on operational processes.

4.4 Response Mitigation

4.4.1 Remediation activities need to be performed where possible 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 Corporate Information Security Office must provide oversight, advice and facilitation to the IT Disaster Recovery Planning Community.

5.1.2 The Corporate Information Security Office 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 IT 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 IT 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 Corporate Information Security Office.

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

5.2 Recovery Improvements

5.2.1 A managed IT Disaster Recover 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 Communications plan needs to in place for IT Disaster Recovery. Executive and operational teams need to have the appropriate communications. The CISO is responsible for developing, maintaining, and communicating this plan.

Replaces Existing Policy Instruments

GoA Information Security Management Directives – 2018

Authority

This Directive is approved by the Corporate Chief Information Officer under authority of the Deputy Minister of Service Alberta.

Stephen Bull Digitally signed by Stephen Bull
Date: 2020.03.03 10:25:54 -07'00'

Original signed by ______________________________ Date ______________________

Corporate Chief Information Officer

Glossary of Terms

Application (business application) – a collection of computer programs, databases, and procedures designed to help an GoA perform particular tasks or handle particular types of IT problems by automating a business process or function

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

Audit – is 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 - the act of establishing or confirming something (or someone) as authentic, that is, that claims made by, or about, the thing are true. Authenticating a person often consists of verifying their identity.

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 in order to minimize the impact of change-related incidents and to improve day-to-day operations.

Confidentiality – information is not 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.

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 (Business Continuity Plan or 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 destroy, transfer to the government archives, transfer to inactive records storage space, or retain 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 – is an identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

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

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 including technologies currently in use and future technologies.

Information asset – means 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 Government of Alberta. Government records include machine-readable records, data stored in information systems, film, audio and audiovisual tapes, etc. Government records include 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 information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure. 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 – maintain or administer information resources on behalf of the Information controller. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource.

In contrast, information custody means having physical possession of information without necessarily having responsibility for the information.

Information management - involves the planning, directing and controlling of all of the government's information assets to meet corporate goals and to 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 below for definition).

Information security – the protection of information from a wide range of threats in order 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 - the 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 together 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 Biometric - something the person is.

Operating procedure - tools which implement business processes compliant with policy, 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 behaviors or actions are expected. A policy defines a course of action, set of principles or plan that guides, directs or influences decision making. IMT Policies are set by the Minister of Service Alberta 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 and 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. (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 secure area is 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 – 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 not limited to) application and system software, development tools, 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 party and includes a person 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, business 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.