Organization of Information Security

Last revised: April 2021
Last reviewed: April 2021
Next review: April 2022

Ministry of SaskBuilds and Procurement
Information Technology Division, Information Security Branch

Purpose

The purpose of this policy is to establish a framework to initiate and control the implementation and operation of information security within the government.

Scope

This policy applies to all GoS owned or operated information systems, intellectual property, and government records.

Definitions

This section intentionally left blank.

Governing Laws & Regulations

Guidance	Section
ISO27001:2013	A.6

Policy Statements

All information security responsibilities must be defined and allocated.

The following outlines the organization of information security in the Government of Saskatchewan. Roles, responsibilities, and accountabilities for key positions are described.

Chief Information Security Officer (CISO)

The Chief Information Security Officer is responsible for:

- advising the Minister of SaskBuilds and Procurement and the Deputy Minister of SaskBuilds and Procurement on Government of Saskatchewan information security standards or policies.
- setting government-wide security objectives, standards, and guidelines.
- monitoring compliance at a government-wide level and managing a process for exceptions.
- managing policy instruments according to the principles laid out by the Information Security Branch.
- promote professional certification and membership in professional associations for personnel throughout government that have information security responsibilities.

Manager, Information Security

The Manager, Information Security is responsible for:

- developing the Information Security Program.
- implementing government-wide information security standards and policies.
- coordinating regular reviews of standards and policies for effectiveness and relevancy.
- ensuring standards and policies are consistent with current technology and security requirements.
- representing the CIO and Ministry of SaskBuilds and Procurement on matters pertaining to security.
- maintain appropriate contact with Local, Provincial, and Federal Authorities.

The Manager, Information Security Branch, must ensure that external authorities, emergency support staff, and service providers can be contacted by:

- maintaining and distributing a list of internal and external authorities and service providers.
- documenting emergency and non-emergency procedures for contacting authorities as required during information security incidents or investigations.

Information Security Branch

Information Security Branch within Information Technology Division of the Ministry of SaskBuilds and Procurement is responsible for:

- identifying and mitigating risks to information and information systems within the Government of Saskatchewan.
- providing government with timely and accurate information regarding current and future information security risks as they relate to government service delivery.
- endorsing a service delivery model which focuses on relationship management, security investment planning, compliance, awareness, and training.
- policy development, standards development, and management of the information security portfolio.
- procuring external suppliers for various information security services.

Security Specialists

The Security Specialists in Information Security Branch are responsible for:

- interpreting the Information Security Standards to assist in the delivery of business functions.
- evaluating information security implications of new government initiatives.
- performing information system security risk analysis activities.
- performing information security assessments and reviews.
- evaluating new threats and vulnerabilities.
- investigating information security incidents.
- advising on the information security requirements for documented agreements.
- analyzing and providing advice on emerging information security standards.
- providing information security advice to supported Ministries and agencies.

Security Officers

Each Ministry must have a designated Security Officer who is responsible for:

- ensuring that procedures to support day-to-day security activities are documented in compliance with the Information Security Standards.
- co-ordinating information security awareness and education.
- investigating reported information security events to determine if further investigation is warranted.
- providing up-to-date information on issues related to information security.
- assisting business areas in conducting Threat and Risk Assessments.
- providing advice on security requirements for information systems development or enhancements.
- co-ordinating ministry information security initiatives with cross-government information security initiatives.

- providing advice on emerging information security standards relating to ministry specific lines of business.
- raising ministry security issues to the cross-government Security Officers' Committee.

Security Officers Committee (SOC)

The Security Officers Committee (SOC) must have representation from each Executive Government Ministry. Agencies must also be represented when their IT infrastructure is supported by Information Technology Division. The SOC is responsible for:

- enhancing the overall security posture of the government.
- advising government on security as a business process.
- guiding the development of a security governance framework that incorporates strategies, reporting, standards, policies, training, enforcement, and compliance.
- working with Information Security Branch in the development, review and approval of policies, standards, and guidelines.
- striving to ensure the highest standard of information protection.
- the communication and awareness of information security standards and policy.

Information Owners

Information Owners have the responsibility and decision-making authority for information throughout its life cycle including creating, regulating, restricting, and administering its use and disclosure. Information owners must:

- determine business requirements including information security needs.
- ensure information and information systems are protected commensurate with their value and level of sensitivity.
- define security requirements during the planning stage of any new or significantly changed information system.
- provide and manage security for information assets throughout their lifecycle.
- determine authorization requirements for access to information and information systems.
- approve access privileges for each user or set of users.
- document information exchange agreements.
- develop service level agreements for information systems under their custody or control.
- implement processes to ensure users are aware of their security responsibilities.
- monitor that users are fulfilling their security responsibilities.
- participate in security reviews and/or audits.

Information Owners must reduce the risk of a disruption of information systems by:

- requiring complete and accurate documentation for all information systems.
- requiring that no single individual has access to all operational functions of an information system.
- rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight on critical systems.
- automating functions to reduce the reliance on human intervention.
- requiring that individuals authorized to conduct sensitive operations do not audit those operations.
- requiring that individuals responsible for initiating an action are not responsible for authorizing that action.

- implementing security controls to minimize opportunities for collusion.

Information Technology Division

Information Technology Division (ITD) manages the government's information technology network including its architecture, security, file systems, and physical infrastructure such as computers, storage systems, and mobile devices. ITD also assists clients with the procurement, operation, management, and upgrading of applications.

Information Technology Division must ensure that:

- creating accounts with elevated privileges is documented and approved by an appropriate officer.
- system, service and application administration duties are segregated.
- application development and database administration are segregated.
- the person who uses an account is not the person who created the account.
- no one single person has control over a business process from inception to completion.

Service Owners

Service owners have the responsibility and decision-making authority for:

- Application Management Services.
- Operations.
- Project Management.
- Data Centre Services.
- Network Services.
- Information Security Branch.
- Client Request Services.
- Deployment Services.
- Regional Support Services.
- Remote Support Services.
- Account Management.
- Problem Management.
- Service Desk.

Service Owners must:

- ensure information and information systems are safeguarded in accordance with their value and level of sensitivity.
- provide and manage security for information assets throughout their lifecycle.
- maintain and operate the technical infrastructure on which information systems reside.
- maintain and operate the security infrastructure that safeguards information systems.
- develop service level agreements for information technology assets under their custody or control.

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of information systems.

Information Security Forums and Professional Associations

Appropriate contacts must be maintained with information security forums and related professional associations.

The Government must promote and enhance employee knowledge of industry trends in information security, best practices, new technologies and emerging threats and vulnerabilities.

Personnel with information security responsibilities must maintain currency by:

- participating in information exchange forums regarding best practices, development of industry standards, new technologies, threats, vulnerabilities, early notice of attacks, and advisories.
- maintaining and improving knowledge of information security topics.
- creating a support network with other security specialists.

Information Security in Projects

Information security must be addressed in project management regardless of the type of the project.

Information Owners and Project Managers must ensure that information security risks are identified and addressed as part of a project. This applies to any project regardless of its character, e.g. a project for a core business process, Information Technology or other supporting processes. The project management methods in use must require that:

- information security objectives are included in project objectives.
- an information security risk assessment is conducted at an early stage of the project to identify controls.
- information security is part of all phases of the applied project methodology.

Information security implications must be addressed and reviewed regularly in all projects. Responsibilities for information security must be defined and allocated to specified roles defined in the project management methods.

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

Information Owners must consider the risks associated with the use of mobile devices in unprotected environments. The following are the minimum controls that must be implemented.

The Information Owner must:

- develop, document and implement procedures on the issuance, usage and return of mobile devices.
- ensure that only government-owned or government-managed mobile devices are used on the government network and to store government information.
- ensure all mobile devices are inventoried.
- ensure mobile devices are returned and, where applicable, disposed of in accordance with the Asset Management Policy and Standards.
- ensure that sensitive data on mobile devices is encrypted with approved methods.
- ensure that mobile devices are password-protected and lock automatically after a predetermined number of unsuccessful login attempts or period of inactivity.
- only allow access and storage of information that has a Security Classification of Level A on mobile devices when there is a distinct business requirement.
- ensure software to protect against malicious software is installed and maintained.
- authorize the use of mobile devices during out-of-country travel.

- ensure users are trained on the proper use of mobile devices, associated software and services, and security incident reporting.
- ensure users are informed of and accept the terms and conditions of these standards and related policies.
- ensure all consultants and IT service provider contracts and agreements include clauses which reference this and other security standards and policies.

Users must:

- have authorization from the Ministry or agency to use mobile device(s).
- ensure that mobile devices in his or her care are only accessed by those authorized to do so.
- ensure that mobile devices are password-protected, and the password applied in accordance with the Access Control Security Policy and Standards.
- ensure that mobile devices are not left unattended.
- protect mobile devices from loss, theft, damage and unauthorized access.
- ensure that information that has a sensitivity of Level A is not accessed by or stored on mobile devices unless s/he has received explicit authorization from the Ministry and the Information Owner to do so.
- ensure that all sensitive information transmitted by or stored on mobile devices is encrypted by approved methods.
- backup information stored on all mobile devices in accordance with Ministry standards and policies.
- ensure that information that cannot be stored on the Ministry shared network drive must be saved to media, encrypted by an approved method and transported and stored securely.
- ensure that data on mobile devices are not the only copies that exist.
- ensure that only software authorized for use on the government network is installed.
- ensure that software is installed only by those authorized to do so.
- ensure that sensitive information is not accessed while using mobile devices in a public place (e.g. coffee shop, airport, park).
- immediately report the loss or theft of a mobile device to the user’s supervisor and the Information Technology Division Service Desk.

Appropriate security controls must be implemented to mitigate risks associated with teleworking.

Telework arrangements must be in compliance with the Government of Saskatchewan *Telework Policy* (Human Resource Manual 1104). Before granting permission to enter into a telework arrangement the Ministry must consider:

- the sensitivity of information accessed or stored at the location.
- the physical security at the teleworking location.
- likelihood of unauthorized access at the teleworking location.
- the security of home wired and wireless networks.
- remote access threats.

Mandatory controls are:

- sensitive government information in electronic format cannot be stored at a teleworking site unless it is encrypted with approved methods.

- sensitive government information in hard copy format cannot be stored at a teleworking site unless it is in a locked cabinet.
- teleworking sites where Classification Level A information is stored must be monitored by alarm when vacant.
- only government-issued computers can be used for the processing of government information.
- only approved remote access methods can be used to access the government network.
- at least monthly, government-issues computers must be brought to the primary work site, logged into the network and have patches and updates applied.
- a home wireless network used to access the government network must be secured in accordance Communications and Network Security Policy and Standards.

Non-Compliance

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

Exceptions

In certain circumstances, exceptions to this policy may be allowed based a review and acceptance of risk by the Security Governance Committee. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Branch. Policy exceptions will be reviewed periodically for appropriateness.

Revision History

Version ID	Date of Change	Author	Rationale