Overarching Security Policy

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

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

Purpose

The purpose of this policy is to provide a framework to manage information security for all Government of Saskatchewan (GoS) information systems (including but not limited to all computers, mobile devices, networking equipment, software, and data).

Scope

This policy applies to all of Government of Saskatchewan employees, contractors, vendors or agents granted access to GoS Information.

Definitions

Information Asset: Hardware, software, network infrastructure and all forms of electronic information that has value to GoS.

Information Asset Owner: A Ministry representative responsible for managing risk to business information assets.

Information Classification: Categorizing information assets based on value and sensitivity to provide and appropriate level of protection.

Information Security Incident: Any policy violation or suspicious/unlawful activity that leads to unauthorized access, use, disclosure, modification, or loss of GoS information systems.

PCI/DSS: An information security standard, Payment Card Industry/Data Security Standard, for organizations that process credit cards from major card vendors.

Significant Change: Any change in GoS that could cause a service disruption.

Threat Risk Assessment: Determining the likelihood of a threat exploiting weaknesses in systems that could result in GoS suffering harm.

Policy Statements

Information Asset Owners must ensure:

- Threat Risk Assessments (TRA) are performed any time there is a new initiative/project to GoS or any time there is a significant change in the GoS environment.
- Information assets are classified according to the following classification levels to ensure that the cost of safeguards and level of protection are proportionate to the value of the asset.
    - **Class A**: Could reasonably be expected to cause extremely serious personal or enterprise injury, including: Significant financial loss, Loss of life or public safety, Social hardship, Major political or economic impact.
    - **Class B**: Could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government program, financial loss, legal action and damage to partnerships, relationships, and reputation.
    - **Class C**: Could reasonably be expected to cause significant injury to individuals or enterprises with limited: financial losses, impact in service/performance levels, and reputation.
    - **Public**: Will not result in injury to individuals, governments, or private sector institutions.

- A risk register is maintained and reviewed annually to ensure that GoS's security posture is always maintained at an acceptable level.
- Information systems that store, process, or transmit GoS information, are protected against unauthorized access, modification and loss in accordance with its information classification level.
- Information systems are monitored at a level consistent with its sensitivity as reflected by its information classification.
- Security patches and software versions are kept up to date on all GoS computers and devices that process or store GoS information. (Refer to Operations Security Standard).
- All Payment Card Industry Data Security Standard (PCI DSS) related activities are outsourced to a PCI compliant vendor.

All users of GoS systems must:

- Comply with the GoS Information Security policy and security standards.
- Protect GoS Information in a manner consistent with the information classification level.
- Access sensitive information only if there is a legitimate business need.
- Report Information Security Incidents immediately to the Information Technology Division Service Desk at: 306-757-5000.

Foundational Security Principles

Principles provide an anchor for building security programs and are intended to guide security decisions. A successful implementation of information security embodies the following principles:

- Central coordination of IT security allows for the proper development of enterprise solutions and monitoring.
- Information Security will be practiced through a unified enterprise approach across government, which will create efficiencies and decrease costs through the creation of economies of scale and scope.
- Using modern, fit-for-use security and information protection technologies for the enterprise.
- Information Security processes and procedures will be readily adaptable to react to technology changes and unexpected events.
- Security is everyone's responsibility.
- Security must reflect asset value and risk.
- Security requires a multi-layered defense strategy.
- System and data access privileges must match job function.
- Security is only as strong as the weakest link.
- Security follows the principles of "least privilege" and "separation of duties" with regard to performing security functions.
- Access to and transmission of data or resources should be secured, audited and monitored at a level consistent with its sensitivity as reflected by its data classification.
- Any individual or service accessing sensitive data or resources, as defined by security policy and data classification, as well as legislative, regulatory and contractual requirements, should be positively identified.
- The recipient of sensitive data is responsible for maintaining the security of the data.

- The implementation of security controls is founded upon a solid understanding of information security requirements, threat and risk assessment, and risk management.
- Security will reduce the implementation time for projects by utilizing a common set of authentication, authorization, and encryption technologies and methodologies for new projects (application and infrastructure).
- Information security policy, objectives, and activities reflect and enable business objectives.

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
1.0	July 26, 2021	Kelsey Sproat	Added Foundational Security Principles as overarching principles.