Overarching Security Policy

Information Security Branch, Ministry of Central Services

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

GoS Overarching Information Security Policy as authorized by the Chief Information Officer.

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 Owner:** A Ministry representative responsible for managing risk to business information assets.
- **Information Asset:** Hardware, software, network infrastructure and all forms of electronic information that has value to GoS.
- **Information security incident:** Any policy violation or suspicious/unlawful activity that leads to unauthorized access, use, disclosure, modification, or loss of GoS information systems.
- **Threat Risk Assessment:** Determining the likelihood of a threat exploiting weaknesses in systems that could result in GoS suffering harm.
- **PCI/DSS:** An information security standard for organizations that process credit cards from the major card vendors.
- **Information Classification:** Categorizing information assets based on value and sensitivity to provide and appropriate level of protection.
- **Significant Change:** Any change in GoS that could cause a service disruption.

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 maintained at an acceptable level at all times.
- 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. (Refer to ***Operations Security Standard***).
- 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.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS 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 on demonstrated business need. Exceptions to this Policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.