Overarching Security Policy - One Government Cyber Program

Last revised: March 11, 2025
Last reviewed: March 11, 2025
Next review: September 2025

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Purpose

The purpose of this policy is to provide strategic guidance and a common standard for information security. Given the seriousness of cyber threats posed to governments and connected entities (Entities), an appropriate threshold of security capability must be met across the Provincial Government. Entities should leverage the principles and domains contained within this policy to build out their cybersecurity program and capabilities to prevent, detect, and respond to information security threats.

This would require entities to develop their own cybersecurity policies and standards based on the entity's unique risk and business objectives.

This will improve alignment of government entities with the Government of Saskatchewan (GOS) goal of achieving a consistent, minimum level of cyber security across government.

Scope

This policy applies to all public entities including executive government ministries, Treasury Board Crowns, eHealth and its supported partners, plus Agencies, Boards, Commissions. It also applies to all government procurement. This document was developed in collaboration with Crown Investments Corporation (CIC) and is consistent with the cybersecurity practices and policies adopted in the CIC Crown Sector.

Guiding Principles

The security principles are grouped into five key activities:

- **Governance** – Develop an organizational understanding to manage security risk to systems, people, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a security event.
- **Respond** – Develop and implement appropriate activities to respond to detected security incident.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities impaired due to a security incident.

Security Program Capability

- To realize desirable outcomes, an Entity must maintain a security program with appropriately robust information security capabilities across all domains and fulfil the Governance Objectives and Operations Objectives listed below.
- For more detail, the Cyber Security and Risk Management Branch of the Ministry of SaskBuilds and Procurement has resources and artifacts that can be leveraged. Please contact *CSITInformationSecurityBranch@gov.sk.ca* and reference this document.

Governance Objectives

- The Entity's information security capabilities shall fulfil the following Governance Objectives:

Domain	Objective
Information Security Program	To define a target state for information security and governance structure that reflects the expectations and requirements of key stakeholders.
Organizational Structure	To manage information security within the Entities, security activities shall be co-ordinated by representatives from different parts of the Entity with relevant roles and job functions.
Security Culture and Awareness	To establish a security awareness and training program and develop and communicate information security policies including acceptable use policies.
Security Risk Management	To develop a security risk management program that integrates with enterprise-level risk management programs or practices.
Security Policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Security Compliance Management	To avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security policies.
Security Audit	To ensure compliance of systems with Entity's security policies, standards, and maximize the effectiveness of those policies and standards.
Configuration and Change Management	To control changes to information systems by ensuring review and approval from important stakeholders, including information security oversight, prior to implementation.
Human Resource Security	To establish policies and processes that ensures employees and contractors understand and fulfill their security responsibilities.
Security Metrics	To define metrics to measure the effectiveness of the security program and communicate to relevant stakeholders and the Entity's governing bodies.

Operations Objectives - Protect, Detect, Respond, and Recover

Domain	Objective
Protect	
Identity and Access Management	To prevent unauthorized access to operating systems by assigning a unique identifier (user ID) for all users with suitable authentication techniques aligned with the sensitivity of the information being accessed.
Information Asset Management	To achieve and maintain appropriate protection of organizational assets.
Data Security & Privacy	To ensure information protection and privacy as required in relevant legislation, regulations, and, if applicable, contractual clauses.
Network Security	To ensure the protection of information in networks and the protection of the supporting infrastructure.

Domain	Objective
Session Management	To protect endpoint sessions by limiting unsuccessful login attempts and locking out sessions after predetermined periods of inactivity.
Malicious Code Protection	To implement malware protection on endpoints and appropriate gateways and to prevent errors, loss, unauthorized modification, or misuse of information in applications.
Application Security Lifecycle	To Ensure applications are developed, deployed, and maintained in secure manner by using application development life cycle best-practices.
Vulnerability Management	To reduce risks resulting from exploitation of published technical vulnerabilities.
Cryptography Management	To protect the confidentiality, authenticity, or integrity of information by cryptographic means.
Physical Security	To prevent unauthorized physical access, damage and interference to the Entity's premises and information assets
Vendor Risk Management	To ensure third parties have implemented and maintain a level of information security and service delivery in line with the Entity's policies.
Cloud Security	To protect information in the cloud based on the information classification level across environments.
Information Classification	To ensure information assets are classified according to Entity's information classification policy
Detect	
Security Threat Detection	To implement processes and technologies to identify and detect threats before they are exploited
Log and Event Management	To ensure all information processing facilities generate audit and security logs, and that these logs are centrally collated through an event management system to aid security operations monitoring.
Respond	
Security Incident Management	To ensure that policies, processes, and plans are in place to respond to a cyber security incident.
Security e-Discovery and Forensics	To develop the capabilities to collect and preserve forensic and e-discovery information to support forensic investigation and incident response
Recovery	
Backup and Recovery	To maintain the integrity and availability of information and information processing facilities.
Information Security in Business Continuity Planning	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Minimum Security Requirements

A minimum-security program rigor must be established across the GOS environment in order to meet the challenges and risks that cybersecurity can bring. Entities should ensure that:

- A Security Awareness and Training Program is implemented.
- Security resources are engaged any time there is a new initiative/project, or anytime there is a Significant Change in the Entity's environment. When appropriate, based on business impact and information classification, a Threat and Risk Assessment (TRA) is performed.
- A cyber security risk register is maintained and reviewed for adequate mitigation at least annually.
- Information assets are monitored and protected at a level consistent with their sensitivity as reflected by the information classification level.
- Hardware and software versions are maintained at supported levels on all the Entity's information assets that process, store, or transmit the Entity's information. Security patches are applied based on criticality and, for vulnerabilities which cannot be patched, appropriate mitigations are implemented.
- Entities accepting credit card payment shall maintain compliance with the requirements outlined in the Payment Card Industry Data Security Standards (PCI-DSS). All PCI-DSS related activities are conducted by a PCI compliant vendor.
- A threat detection and security incident response program is implemented.
- Security responsibilities for the Entity must be assigned to roles. Accountability for implementing an organizational security program is established.
- Entities with separate IT and Operational Technology environments should implement appropriate network segmentation between the IT and OT environments as recommended in IEC 62443 framework.

Entities should ensure that all users of their systems:

- Comply with the Entity's Information Security policies and security standards.
- Protect the Entity's information assets in a manner consistent with the Entity's information classification level and in accordance with established access control policy.
- Access sensitive information assets only if there is a legitimate business need.
- Report information security incidents immediately to the Entity's support desk or, as is applicable, in accordance with the Entity's cyber security incident response plan.

In certain circumstances, exceptions to the policy may be allowed based on a review and acceptance of risk by the applicable Entity's governing body. Exceptions should be formally documented and approved by the entity's governing body and reviewed at least annually for appropriateness.