# Executive Government Security policy

Last revised: June 2024
Last reviewed: June 2024
**Next review: June 2025**

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

## Purpose

The purpose of this policy is to provide direction and a common standard for Government of Saskatchewan (GoS) entities in building appropriately robust cybersecurity capabilities to prevent, detect, and respond to information security threats.

Given the seriousness of cyber threats posed to governments and connected entities, a certain minimum standard of security capability must be met, while also providing for each entity to meet that standard according to their unique risks and means.

Polices that go beyond the minimum requirements are encouraged.

Additional information about the implementation of these capabilities can be found in the GOS security standards and other policy instruments

## Policy Scope

In accordance with the 'One Government' approach, this policy applies to all Government of Saskatchewan employees, contractors, vendors, or any other agents granted access to the Organization's Information Assets.

This policy applies to all Government of Saskatchewan information systems including but not limited to all Operational Technology (OT) systems, IoT devices, computers, mobile devices, networking equipment, software, and data.

## 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:

- Security is everyone's responsibility.
- 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 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 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.



Government of Saskatchewan

## Minimum Security Requirements

In addition to fulfilling the broad security program objectives above, a minimum-security program rigor must be established. Information Asset owners must ensure that:

- A Security Awareness and Training program is implemented.
- Threat and Risk Assessments (TRA) are performed any time there is a new initiative/project, or any time there is a Significant Change in the Organization's environment.
- A risk register is maintained and reviewed annually to ensure that the Organization's security posture is always maintained at an acceptable level.
- Information Assets which store, process, or transmit the Organization's information are protected against unauthorized access, modification, and loss in accordance with its information classification level.
- Information Assets are monitored at a level consistent with their sensitivity as reflected by the information classification level.
- Security patches and software versions are kept up to date on all of the Organization's Information Assets that process, store, or transmit the Organization's information.
- All Payment Card Industry Data Security Standard (PCI-DSS) related activities are conducted by a PCI compliant vendor.
- A security incident response and threat detection program must be implemented.
- Security responsibilities for organizations must be assigned to roles.

All users of the Organization's systems must:

- Comply with the Organization's Information Security policies and security standards.
- Protect the Organization's Information Assets in a manner consistent with the information classification level.
- Access sensitive Information Assets only if there is a legitimate business need.
- Report Information Security Incidents immediately to the Organization's IT Service Desk.

## Security Program Capability Objectives

In order to realize our mission statement, organizations must maintain a security program with appropriately robust capabilities across all domains, which apply the Foundational Security Principles and fulfil the following objectives:

If you want to go into more detail, Government's Cyber Security Branch have resources and artifacts that you may take advantage of. Please contact *CSITInformationSecurityBranch@gov.sk.ca*

## Governance

| 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 organization. Security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions |
| Security Culture and Awareness | To establish a security awareness and training program and develop and communicate 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 requirements. |
| Security Audit | To ensure compliance of systems with organizational security policies and standards and maximize the effectiveness of and minimize interference to/from the information systems audit process. |

## Operations

| Domain | Objective |
|---|---|
| Identity and Access Management | To prevent unauthorized access to operating systems by assigning a unique identifier (user ID) for all users and choosing a suitable authentication technique to substantiate the claimed identity of a user. |
| Information Asset Management | To achieve and maintain appropriate protection of organizational assets. |
| Data Security & Privacy | To ensure data 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. |
| Endpoint Security | 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 practices such as DevSecOps |
| 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 organization's premises and information. |
| Human Resource Security | To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. |
| Configuration and Change Management | To control changes to information by reviewing and approving prior to implementation. |
| Vendor Risk Management | To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. |
| Cloud Security | To protect data in the cloud based on the data classification level across environments. |

| | |
|---|---|
| Security Threat Detection | To implement a process by which you find threats on your network, your systems or your applications and to detect threats before they are exploited as attacks. |
| Log and Event Management | To provide the capability to detect events, make sense of them and determine the appropriate control action. This is the basis for operational monitoring and control. |
| Security Incident Management | To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. |
| Security e-Discovery and Forensics | To collect forensic and e-discovery data and preserve as required in support of forensic investigations. |
| Backup and Recovery | To maintain the integrity and availability of information and information processing facilities. |
| InfoSec 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. |
| Security Metrics | To define metrics to measure the effectiveness of the security program and communicate to relevant stakeholders. |
| Data Classification | Information assets are classified according to GIP defined classification levels, to ensure that the cost of safeguards and level of protection are proportionate to the value of the asset. |

## 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. |
| 2.0 | June 23, 2022 | Kelsey Sproat | Total revision for annual update. |
| 3.0 | June 24, 2024 | Arnold Duze | Reviewed. Renamed to Executive Government Security Policy. |
| | | | |
| | | | |