Internal Security Governance Policy

Ministry of SaskBuilds and Procurement
Information Technology Division (ITD)
Cyber Security and Risk Management Branch (CSRM)

Last revised: October 2023
Last reviewed: October 2023
Next review: October 2024

Internal Security Governance Policy

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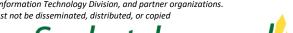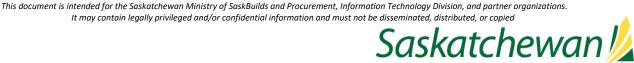Information Technology Division, Cyber Security and Risk Management Branch

Contents

This document is intended for the Saskatchewan Ministry of SaskBuilds and Procurement, Information Technology Division, and partner organizations.
It may contain legally privileged and/or confidential information and must not be disseminated, distributed, or copied

Internal Security Governance Policy

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

Purpose

The purpose of this policy is to ensure that a governance strategy and process is in place for all Internal Security Policies to follow as part of their lifecycle. This policy follows ISO 27000 industry standards for controls and the governance elements required.

Scope

This Internal Security Governance Policy applies to all internal security policies with respect to the governance, creation, approval process, and lifecycle management of all the Security Policies that are identified and in use by the Government of Saskatchewan. This Internal Security Governance policy was created as the governance control for all Security Policies and is aligned with ISO 27000 Industry Standards.

Governing Laws, Regulations, and Standards

Resource	Description
Privacy Act	*P-21.pdf (justice.gc.ca) Government of Canada Privacy Act*
PIPEDA	*P-8.6.pdf (justice.gc.ca)Government of Canada PIPEDA Act*
Freedom of Information and Protection of Privacy Act	Saskatchewan's provincial public sector privacy law
Local Authority Freedom of Information and Protection of Privacy Act	*Saskatchewan's municipal public sector privacy law*
Health Information Protection Act	*Saskatchewan's privacy law relating to health records*
ISO/IEC 27001:2013	A.5 (A.5.1, A.5.1.1, A.5.1.2)
ISO/IEC 27002:2022	5.1,5.2,5.3,5.4
NIST (National Institute of Standards and Technology) SP 800-53 r5	AC-1,AT-1,AU-1,CA-1,CM-1,CP-1,IA-1,IR-1,MA-1,MP-1,PE-1,PL-1,PM-1,PS-1,PT-1,RA-1,SA-1,SC-1,SI-1,SR-1

Policy Statements

- The Government of Saskatchewan must maintain a set of Security Policies for information security and can be issued in a single "information security policy" document or as a set of individual but related documents.
- All Government of Saskatchewan Security Policies must be approved by Management in consultation with the Executive Management.
- These policies must be communicated to employees, contractors, and relevant external parties in a form that is relevant, accessible, and understandable to the intended reader using security awareness sessions or other educational training programs.
- Government of Saskatchewan security policies must be reviewed at planned intervals, (annually) or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
- Government of Saskatchewan security policies are owned by the Cyber Security and Risk Management Branch management team of the Information Technology Division within the SaskBuilds and Procurement ministry.
- All Government of Saskatchewan security policies must have details specifying Non-Compliance and Exception management conditions.
- The use of the term MUST implies a mandatory requirement, whereas the term of SHOULD is a suggested item for all policies.

Supporting Internal Resources

This table provides a list of all current security policies that are in place for the Government of Saskatchewan.

Resource	Description
Overarching Information Security Policy	All Government of Saskatchewan Security Policies align to this overarching Policy and provide a means of supporting this policy.
Access Control Policy	Access Control Policy for all employees, contractors and interfaces used by Government of Saskatchewan.

Non-Compliance

In cases where it is determined that a breach or violation of Government of Saskatchewan Information Security policies has occurred, the respective Ministry under the direction of the Chief Information Officer and Information Security Branch, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, in accordance with PS 803 Corrective Discipline policy, 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 Security Officer, under the guidance of the Cyber Security and Risk Management Branch. Policy exceptions will be reviewed periodically for appropriateness.

Definitions

ISO/IEC – International Standards Organization / International Electrotechnical Commission

NIST - National Institute of Standards and Technology

Revision History

Version ID	Date of Change	Author	Rationale
V0.1	10 March 2023	CSRM	Initial Draft
V1.2	25 October	CSRM	Final Review

Saskatchewan