Security Compliance Policy

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

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

Security Compliance Policy

Ministry of Sask Builds and Procurement
Information Technology Division,
Cyber Security & Risk Management Branch

Contents

Security Compliance Policy

Ministry of Sask Builds and Procurement
Information Technology Division,
Cyber Security & Risk Management Branch

Purpose

The purpose of this policy is to ensure proper measures are in place to avoid non-adherence to information security compliance requirements with respect to – legal, statutory, regulatory, and contractual or otherwise. This policy defines governing regulations, internal and industry standards required to access Government of Saskatchewan assets.

Scope

This Security Compliance Policy applies to all business processes and data, information systems, components, personnel, and physical areas of the Government of Saskatchewan. Person(s) this policy applies to include but are not limited to:

- All employees, whether employed on a full-time or part-time basis by the Government of Saskatchewan
- Contractors and Service Providers that access and manage Government of Saskatchewan assets and information.

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*
Archives and Public Management Act	*The Archives and Public Management Act, 2015*
ISO/IEC 27001:2013	A.18 (A.18.1, A.18.2)
ISO/IEC 27002:2022	5.31, 5.32
NIST (National Institute of Standards and Technology) SP 800-53 v4	XX-1 controls, CM-10, AC-3, AU-9, AU-11, CP-9, MP-4, SA-5, SI-12, Appendix J Privacy Controls, SI-12, AC-8, AU-6, CM-11, PL-4, PS-6, PS-8, IA-7, SC-13, CA-2, CA-7, RA-5, AU-1, AU-2, SI-4
NIST CSF	ID. GV-3

Security Compliance Policy

Ministry of Sask Builds and Procurement
Information Technology Division,
Cyber Security & Risk Management Branch

Policy Statements

- The Government of Saskatchewan must ensure compliance with legal, statutory, regulatory, and contractual requirements related to information security assets management.
- The Government of Saskatchewan must maintain controls, policies and procedures, risk assessments, and auditing along with verification of vendors compliance to said items, that provide services that can impact information assets.
- All vendors and service providers must be complying to Appendix G of all RFP – RFR or any services provided that is part of a public program submission.
- The Government of Saskatchewan must validate that cryptography has been implemented in accordance with the cryptography policy and standards for all required classes of data as specified in the IPSC Information Protection Security Controls guideline.
- The Government of Saskatchewan must maintain compliance with all areas as it relates to intellectual property rights and use of proprietary products.

Supporting Internal Resources

Resource	Description
Internal Security Governance Policy	All Government of Saskatchewan Security Policies align to this Governance Policy
Information Protection Security Controls (IPSC) for Classified Data	This document defines the required access controls required to provide the proper security based on Classified Data for Government of Saskatchewan
Cryptography Policy/Standard	This document defines the required cryptography standards that are required the Government of Saskatchewan assets
Appendix G – RFP -RFR Vendor Agreements	Vendors must be complying to this appendix is required for all vendor service that are submitted to market for systems, resources, and/or services.

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

This section intentionally left blank.

Revision History

Version ID	Date of Change	Author	Rationale
V1.1	03 October 2023	CSRM	Updated removing standards and specifications, referencing external documents
V1.2	25 October 2023	CSRM	Final Review