Cryptography Security Policy

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

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

Cryptography Security Policy

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

Contents

PURPOSE 2
SCOPE 2
GOVERNING LAWS, REGULATIONS, AND STANDARDS 2
POLICY STATEMENTS 3
SUPPORTING INTERNAL RESOURCES 3
NON-COMPLIANCE 4
EXCEPTIONS 4
DEFINITIONS 4
REVISION HISTORY 4

Cryptography Security Policy

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

Purpose

The purpose of this policy is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory, and contractual requirements related to cryptography. This policy defines governing regulations, internal and industry standards required to address cryptography for Government of Saskatchewan assets.

Scope

This Cryptography 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.

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.10 (A.10.1)
ISO/IEC 27002:2022	8.24
NIST (National Institute of Standards and Technology)SP 800-53 v4	SC-12, SC-13, SC-17
NIST SP 800-171	2.1, 3.6

Cryptography Security Policy

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

Policy Statements

- The Government of Saskatchewan must use cryptography to provide the confidentiality, authenticity and integrity while protecting sensitive data and access to assets within the ministries.
- The Government of Saskatchewan must use cryptographic technologies that are in alignment with the Government of Saskatchewan Cryptographic Standard.
- The Government of Saskatchewan must ensure that cryptographic requirements are defined based on risk for users, processes, information assets and devices.
- The Government of Saskatchewan must have specific cryptographic controls based on the classification of the data that is being managed. (i.e.: Information Protection Security Controls IPSC)
- The Government of Saskatchewan must comply with the CP/CPS Policy/Standard when issuing and managing PKI (Public Key Infrastructure) certificates.
- All access to systems via API (Application Programming Interfaces), machine to machine or other interface mechanisms must conform to the cryptographic policy and cryptographic standards to provide the required level of encryption needed to protect the information and assets.

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 to be used for the Government of Saskatchewan assets
Wireless Access Standard	This document defines the required controls that are required to deliver access to the Government of Saskatchewan Wireless Networks
CP/CPS PKI Policy/Standard	The CP/CPS PKI Policy/Standards document provides addition details as to specific key management governance, key standards and PKI key specification.

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
V1.0	11 April 2023	CSRM	Updated removing standards and specifications, referencing external documents
V1.1	11 April 2023	CSRM	Updated Header, added IPSC and CP/CPS references
V1.2	29 May 2023	CSRM	Add 3rd party recommended changes
V1.2	25 October 2023	CSRM	Final Review