Cryptography Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Information Security Branch

Last revised: April 2021
Last reviewed: April 2021
Next review: April 2022

Purpose

The purpose of this policy is to ensure the correct use of cryptography to protect the confidentiality, authenticity, and integrity of The Government of Saskatchewan's information.

Scope

This Cryptography Policy applies to all business processes and data, information systems and components, personnel, and physical areas of The Government of Saskatchewan.

Definitions

This section intentionally left blank.

Governing Laws & Regulations & Standards

Guidance	Section
ISO27001:2013	A.10 (A.10.1)
NIST SP 800-53 v4	SC-12, SC-13, SC-17
NIST SP 800-21	2.1, 3.6

Policy Statements

Cryptographic Controls:

- The Government of Saskatchewan will develop a policy surrounding the proper procedures needed around the use of cryptographic controls. The following items should be considered:
    - Based on a risk assessment, the required level of protection should be identified considering the type, strength, and quality of the encryption algorithm required.
    - The use of encryption for the protection of information transported by mobile or removable media devices or across communication lines.
    - The standards to be adopted for effective implementation throughout the organization.
    - The impact of using encrypted information on controls that rely upon content inspection.

Key Management:

- Cryptographic keys should be protected through their whole lifecycle.
- Cryptographic algorithms, key lengths, and usage practices should be selected according to best practice.
- All cryptographic keys should be protected against modification and loss. Also, secret, and private keys need protection against unauthorized use as well as disclosure.
- Equipment used to generate, store, and archive keys should be physically protected.
- A key management system should be based on an agreed set of standards, procedures, and secure methods for:
    - Generating keys for different cryptographic systems and different applications.
    - Issuing and obtaining public key certificates.
    - Distributing keys to intended entities, including how keys should be activated when received.
    - Storing keys, including how authorized users obtain access to keys.

- Changing or updating keys, including rules on when keys should be changed and how this will be done.
- Dealing with compromised keys.
- Revoking keys, including how keys should be withdrawn or deactivated.
- Recovering keys that are lost or corrupted.
- Backing up or archiving keys.
- Destroying keys.
- Logging and auditing of key management related activities.

Relevant Procedures

This section intentionally left blank.

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 acceptable 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