Cryptography Security Policy

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security policy for Cryptography.

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality and integrity of government information.

Scope

This policy applies to all GoS use of cryptography and cryptographic keys.

Policy Statements

The use of cryptographic controls must be based on the risk of unauthorized disclosure and the sensitivity of the information or information system that is to be protected.

The Chief Information Security Officer provides government direction and leadership in the use of cryptography and the provision of cryptographic services (e.g. user registration services, key management) by:

- establishing policy and standards and providing strategic direction on the use of cryptography;
- setting security standards for cryptographic algorithms and key length; and
- approving the use of cryptographic services.

The Executive Director, Information Security Branch, supports the use of cryptography in government by:

- defining and maintaining standards for cryptographic controls; and
- providing technical advice on the use of cryptography.

A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls. The Chief Information Security Officer is responsible for approving key management standards and processes including:

- selection and length of cryptographic keys;
- generation of keys;
- generation and distribution of public key certificates;
- distribution, storage and periodic updating of keys;
- revocation of keys (e.g. when a user changes role);
- recovery of keys that are lost, corrupted or expired;
- management of keys that may have been compromised;
- archiving keys and the maintenance of key history; and
- allocation of activation/de-activation dates.

Compliance and Disciplinary Action

In cases where it is determined that a breach or violation of GoS 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 on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.