Cryptography Security Specifications

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 specifications for Cryptography.

Table of Contents

Reference Documents

The following documentation is available on the IT Security Services Taskroom:

- *Cryptography Security Policy*
- *Cryptography Security Standard*

1. General

Cryptographic modules, cryptographic software, and hardware used to safeguard sensitive government information must be validated to FIPS 140-2 standards.

These are products or cryptographic modules validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in Federal Information Protection Standard (FIPS) 140-2 (as amended). Validated modules are approved for the protection of Sensitive Information in the US Government and Protected Information in the Government of Canada.

You may refer to the *US National Institute of Standards and Technology (NIST)* discussing CMVP.

2. USB Drives

USB drives used to store sensitive government information must be protected against unauthorized access, loss and theft. A device chosen for this purpose must meet the following requirements:

- it uses hardware-based encryption;
- device is Validated to at least FIPS 140-2 Level 2;
- all user-writable drives on the device are fully encrypted;
- the encryption algorithm is AES-256;
- the device must be configured with a complex password that meets the minimum password standard described in ***Access Control Security Standards***, Section 3.1.1, Password Standards;
- the device must be configured to lockdown and destroy the encryption key after a maximum of ten failed login attempts.

Contact Information Security Branch for current products that meet these requirements and are available to government users through normal procurement channels.

Email: *ITOInformationSecurityBranch@gov.sk.ca*

3. External Hard Drives

External hard drives used to store sensitive government information must be protected against unauthorized access, loss and theft. A device chosen for this purpose must meet the following requirements:

- it uses hardware-based encryption;
- device is Validated to at least FIPS 140-2 Level 2;
- all user-writable drives on the device are fully encrypted;
- the encryption algorithm is AES-256;
- the device must be configured with a complex password that meets the minimum password standard described in ***Access Control Security Standards***, Section 3.1.1, Password Standards;
- the device must be configured to lockdown and destroy the encryption key after a maximum of ten failed login attempts.

Contact Information Security Branch for the current recommended products that meet these requirements and can be procured through normal channels.

Email: *ITOInformationSecurityBranch@gov.sk.ca*

4. Windows Laptops Hard Drive Encryption

Government laptops are sometimes used outside the security zones of government buildings. The content on their hard drives must be safeguarded against unauthorized access, loss and theft. The following security controls must be applied:

- all drives are safeguarded with full disk encryption;
- the encryption algorithm is AES-256;
- the encryption product used is validated to at least FIPS 140-2 Level 2;
- the user password must be complex and meet the minimum standards in accordance with ***Access Control Security Standards***, Section 3.1.1, Password Standards.

Contact Information Security Branch for current products that meet these requirements and can be procured through normal channels.

Email: *ITOInformationSecurityBranch@gov.sk.ca*

5. Secure Shell (SSH) and Secure File Transfer Protocol (SFTP)

SSH is used by system administrators as a means of remotely managing and configuring a variety of hosts. SFTP is based on SSH and is implemented as a means of securely transferring files between hosts. Software solutions must be configured as follows:

- use SSH version 2;
- do not use host-based authentication;
- the LoginGraceTime must be set to a maximum of 120 seconds;
- the use of .rhosts and .shosts user files must be disabled;
- login via root is not permitted if the system is directly accessible via the internet;
- disable logging into accounts with empty passwords;
- the encryption algorithm must be AES with a minimum key length of 256 bits;
- the Message Authentication Code (MAC) must use a hash algorithm with 256 bits or stronger; and
- contact Information Security Branch for a government-authorized login banner.