Asset Management Security Standard

Information Security Branch, Ministry of Central Services

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

This document outlines the Government of Saskatchewan security standards for Asset Management.

Table of Contents

Reference Documents

The following documents are available on the IT Security Services Taskroom:

- *Asset Management Security Policy*

Government of Saskatchewan

1. Business Requirements of Access Control

1.1. Responsibility for Assets

Information Owners and Service Owners must identify and document assets under their control including:

- software (e.g. applications, system software, development tools and utilities);
- hardware (e.g. computer and communications equipment, removable media, etc.);
- services (e.g. computer and communications services, general utilities); and
- information assets and their security classification.

Information assets include databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails and archived information.

The following information must be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss or destruction:

- type of asset;
- ownership;
- format;
- location;
- assigned user (where applicable);
- backup information;
- license information;
- security requirements (confidentiality, integrity and availability); and
- consequence of loss.

1.2. Return of Assets

Managers must ensure the recovery of:

- documents, files, data, books and manuals in electronic and hard copy formats;
- information assets developed or prepared by an employee or contractor in the course of his/her duties;
- work-related email in the current and archived mailboxes;
- computer hardware, software and related equipment;
- mobile devices and portable media; and
- access cards, keys, key fobs, id cards and other government-issued devices.

The user must copy all **personal** electronic files to removable media and delete the originals from government systems.

Unreturned access devices must be documented and steps taken to ensure they cannot be used for unauthorized access to Government building, information systems and/or data.

The ***Employee Services Centre*** includes manager checklists to be used when an employee is terminated.

2. Information Classification

2.1. Classification of Information

The Information Technology Division is responsible for developing an information classification system. The system must take into account the confidentiality, integrity, and availability requirements and the financial value of information assets.

The Government of Saskatchewan's information classification levels are:

- **A: high sensitivity** – unauthorized disclosure could cause extreme injury to government or a person;
- **B: medium sensitivity** – unauthorized disclosure could cause serious injury to the government or a person;
- **C: low sensitivity** – unauthorized disclosure could cause low injury to the government or a person;
- **Public: non-sensitive** – unauthorized disclosure will not result in injury to the government or a person.

Information owners must assign a level of sensitivity in accordance with the ***Guide for Information Protection Classification***. The guide includes more details of the classification levels and examples. In determining the level of sensitivity information owners must consider that, in some cases, the aggregate of the information can be more sensitive than a smaller subset or individual record. In addition, some information is only sensitive for a certain period of time and the classification level may change accordingly.

2.2. Labelling of Information

Information Owners must ensure that information, whether in physical or electronic format, is labeled with its information security classification. This communicates to information users the level of sensitivity and required safeguards.

Items for consideration include printed or electronic records, reports, files, on-screen displays, recorded media and messages.

Automated labeling must be used where available such as document templates, headers and footers, and selectable boxes in forms. Where labeling is not feasible an alternate method must be used, e.g. marking storage media, written procedures or metadata.

Information Owners must establish handling procedures for the secure processing, storage, transmission, declassification and destruction of information and digital media.

Agreements with other governments and organizations that include information sharing must include procedures to identify the level of sensitivity of the information and interpret the classification labels from external partners.

2.3. Handling of Assets

Information Owners and Service Owners must develop and implement procedures for handling, processing, storing and communicating information. Those procedures must consider:

- the level of sensitivity of the information;
- access restrictions supporting the safeguards for each level of sensitivity;
- maintenance of a formal record of the authorized recipients of assets;
- safeguarding temporary or permanent copies to a level consistent with the original;

- storage of information technology assets in accordance with the manufacturers' specifications; and
- clear marking of all copies of media for the attention of the authorized recipient.

Agreements with other governments and agencies that include information sharing must also include:

- identification of the classification of that information; and
- interpretation of the classification labels from other agencies.

3. Media Handling

3.1. Management of Removable Media

Information Owners and Service Owners must:

- ensure that sensitive data on removable media is encrypted with approved methods;
- authorize the use of removable media during out-of-country travel;
- ensure users are familiar with the operation of removable media;
- ensure users are familiar with the standards and policies on security incident reporting; and
- ensure all users who are authorized to use removable media are aware of the need to safeguard government information in accordance with these standards and related policies.

Users of removable media must:

- have authorization from the Ministry to use removable media and store sensitive information on it;
- ensure that removable media in his or her care is only accessed by those authorized to do so;
- ensure that, where applicable, the media is password-protected and the password applied in accordance with relevant Policies and Standards;
- ensure that removable media is transported securely and not left unattended;
- ensure that sensitive information stored on removable media is encrypted by approved methods;
- ensure that data on removable media are not the only copies that exist, i.e. originals are on network shares;
- ensure that any removable media received from an external party is scanned for malware prior to use;
- ensured that any removable media received from a foreign country is first screened by Information Security Branch before connecting it to a government computer;
- ensure that removable media is not used for the storage of sensitive information when encryption is not available, e.g. storage card on a digital camera;
- ensure that sensitive information is not accessed while in a public place (e.g. coffee shop, airport, park); and
- immediately report the loss or theft removable media to the user's supervisor and the Information Technology Division Service Desk.

3.2. Disposal of Media — Media Sanitization Standard

The Government of Saskatchewan standard for media sanitization is:

- US Department of Defense DoD 5220.22-M

Contact Information Security Branch for products that comply with this standard.

3.3. Physical Media Transfer

When transporting physical media with sensitive information between sites:

- use a trusted courier;
- inspect the identification of couriers at pickup and delivery;
- obtain and retain receipts;
- pack the media in a manner that will prevent loss or damage;
- pack the media in a manner that does not disclose the level of sensitivity;
- pack it in a manner to make evident any attempted tampering.

When supported by a Threat and Risk Assessment or if enhanced security is required for other reasons:

- use a courier service that has a tracking number;
- hand deliver the media where necessary;
- use a double envelope (or double package) where the inner layer is marked with the level of sensitivity and instructions and it is packaged in another envelope;
- use a lockable container;
- encrypt the information stored on the media.