Asset Management 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 Asset Management.

Purpose

To identify and safeguard government information assets in accordance with their sensitivity and value.

Scope

This policy applies to all GoS information assets and services associated with the governments' information technology.

Policy Statements

To identify government information assets and define appropriate protection responsibilities:

- An inventory of all important assets associated with information systems must be documented and maintained. The inventory must not duplicate other inventories unnecessarily but reference them where appropriate.
- The loss, theft or misappropriation of assets must be reported immediately to the Manager and the Information Technology Division Service Desk. When information is lost, stolen or misappropriated the security policies and procedures relating to "Information Security Incident Management" must be followed.
- Information Owners or Service Owners must be designated for all assets and services associated with the governments' information technology. Information Owners and Service Owners are responsible for:
    - controlling the production, development, maintenance, use and security of information and information assets in their jurisdiction;
    - ensuring that information and information assets are appropriately classified and safeguarded; and
    - defining and regularly reviewing access restrictions and classifications in accordance with applicable standards and policies.
- Rules for the acceptable use of information systems must be identified, documented and implemented:
    - All users of the government's information systems must take responsibility for and accept the duty to actively protect the government's information assets.
    - The requirements for core and incidental use are described in Section 1103 of the Human Resource Manual, **Information Technology Acceptable Usage Policy**.
- Personnel must return government assets upon termination or change of employment.

To ensure that government information receives and appropriate level of protection in accordance with its sensitivity and value:

- Information must be classified in accordance with its value, sensitivity and intended use. Information owners must assign a level of sensitivity in accordance with the **Guide for Information Protection Classification**.
- Information must be appropriately labeled in accordance with the assigned level of sensitivity.
- Information must be appropriately handled in accordance with its assigned level of sensitivity.

To prevent unauthorized disclosure, modification, removal or destruction of government information stored on media:

- All removable computer media must be managed according the relevant Asset Management Standards and appropriate controls applied considering the sensitivity of the data they store.
- Purchasing Branch in Commercial Services Division of the Ministry of Central Services is responsible for preparing and publishing the **Electronic Storage Media Disposal Policy**. Information Owners must ensure that media that is no longer required operationally is disposed of securely and in accordance with the Electronic Storage Media Disposal Policy and the relevant Information Security Standards for media disposal.
- Media being physically transported must be appropriately protected according the relevant Asset Management Standards.

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.