Asset Management Policy

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

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

Purpose

The purpose of this policy is to ensure assets are identified appropriately and the proper protection controls in accordance with their sensitivity and value to The Government of Saskatchewan

Scope

This Asset Management 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, and Standards

Guidance	Section
ISO27001:2013	A.8 (A.8.1., A.8.2., A.8.3.)
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16

Policy Statements

Responsibility for Assets:

- Information or information processing facility assets must be inventoried and documented and that record must be kept up to date.
    - Inventory categorization must be approved by the appropriate parties or authorizing authority.
    - Organization will employ use of automated mechanisms to identify unauthorized systems including hardware or software.
    - Inventory must also include information system updates or removals.
- This process must be assigned to an owner to maintain the process.
    - Information Owners or Service Owners must be designated for all assets and services associated with the government's 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.
        - 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

- The following assets should be considered in the inventory process:
    - Authorized assets
    - Unauthorized assets
    - Software
    - Databases
    - Information stores
    - Physical assets
    - Services
    - People
    - Tangibles
- Processes around configuration management will be established as well.
- All assets must be returned upon termination of employment or contract.

Information Classification:

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

- All assets must be classified in terms of legal requirements, value to the organization, their criticality to the organization, and sensitivity if they were to be disclosed by an unauthorized party.
- The Government of Saskatchewan's data shall 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*.
- Assets will be labeled and handled based on appropriate information classification procedures used by the organization.

Media Handling:

- Removable media must also be managed according to the relevant Asset Management Standards and appropriate controls applied considering the sensitivity of the data they store.
- Removable media must be protected against unauthorized access and misuse while in use and in transit, and must be disposed of securely, using appropriate procedures.
- Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation.
- 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 is no longer required operationally is disposed of securely and in accordance with the Electronics Storage Media Disposal Policy and the relevant Information Security Standards for media Disposal.
- Media being physically transported must be appropriately protected according to the relevant Asset Management Standards.

Acceptable Use:

- Standards or guidelines for the acceptable usage of assets should be documented to indicate what information system users are and are not allowed to do.
- The following items should be covered in acceptable usage guidelines:
    - Computer and information system usage
    - Software and data usage
    - Internet and email usage

    - Telephone usage
    - Office equipment & materials usage

- As a requirement of information system access, and as a component of security awareness training, all information system users, whether employees or third parties, will be required to provide signed acceptance of the acceptable usage guidelines.

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 acceptance 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