1. PURPOSE

To establish the baseline security controls that support the Defensible Security principles and industry best practices for managing physical IT assets, and information assets in order to protect confidential government information and information systems.

2. DESCRIPTION

This standard is designed to be read in conjunction with the Information Security Standard and IT Asset Management Security Guidelines. It provides the definition of an IT Asset, information assets, sets the IT Asset inventory requirements, as well as requirements to identify valuable information assets.

3. AUTHORITY

Core Policy and Procedures Manual – Chapter 6: Procurement, Chapter 8: Asset Management, Chapter 12: Information Management and Information Technology Management, Chapter 15: Security.

4. APPLICATION / SCOPE

This standard applies to all ministries, agencies, boards, and commissions that are subject to the Core Policy and Procedures Manual. It covers physical IT assets, and information assets.

5. REQUIREMENTS

5.1 IT Assets

IT Asset is any valuable component that can contribute to the delivery of an IT product or service.

a. IT Assets MUST have a designated Owner. Owners may delegate the responsibility for the custody of IT Assets to Custodians.

b. IT Asset Owners MUST maintain an accurate IT Asset inventory to document, track and manage IT Assets that meet one or more of the criteria outlined in IT Asset Management Security Guidelines Section 2.1.

c. IT Assets that don't meet the stated criteria but may present unnecessary risk to government MUST also be documented, tracked, and managed in IT Asset inventory.

d. IT Asset inventories MUST be kept up-to-date and MUST be reviewed annually.

e. IT Asset inventory MUST have the following attribute categories:

- Identification attributes
- Owner/responsibility attributes
- Management attributes
- Risk attributes

f. IT Assets MUST have security controls and safeguards appropriate for the classification and type of the asset.

g. Security controls and safeguards appropriate for the classification and type of the asset MUST be applied and maintained throughout the lifecycle of the IT Asset to minimise the likelihood of loss, theft, or damage.

h. IT Assets that contain or store sensitive data MUST be handled in accordance with their Information Security Classification label to minimise the likelihood of an information or security breach.

i. IT Assets MUST be disposed of in accordance with the government disposal process.

j. Access to an IT Asset inventory MUST be limited to authorized personnel.

5.2 Information assets

Information assets are collections of data that are processed, analyzed, interpreted, classified, or communicated in order to serve a useful purpose, present fact, or represent knowledge in any medium or form, that may have financial value and/or is essential in providing a service or in decision-making. In addition to identifying IT Assets, IT Asset Owners MUST also identify the following information assets under their control:

- Software and Services including computer and communications services, cloud-based services and general utilities that involve sensitive and confidential information;
- Information assets required to be inventoried in the personal information directory (required under the Freedom of Information and Protection of Privacy Act); and,
- All other assets involving sensitive and confidential information.

a. Information asset inventories MUST be kept up-to-date and MUST be reviewed annually.

b. Information asset inventories MUST include the relevant attributes.

c. Information assets MUST have security classification and labelling applied in accordance with the Information Security Classification Standard.

d. Information assets MUST have security controls and safeguards appropriate for the security classification and type of asset.

e. Security controls and safeguards appropriate for the classification and type of the asset MUST be applied and maintained throughout the lifecycle of the Information asset to minimise the likelihood of information breach, unauthorised use, loss, theft, or damage.

f. Information assets MUST be handled in accordance with their Information Security Classification label to minimise the likelihood of information breach.

g. Information assets MUST be disposed of at the end of their lifecycle in accordance with their classification, type of asset and records management schedules.

h. Access to an Information and data asset inventory MUST be limited to authorized personnel.

6. SUPPORTING DOCUMENTS

IT Asset Management Security Guidelines

IMIT 6.18 Information Security Classification Standard

Information Security Classification Guidelines

IMIT 6.19 Information Security Standard

Information Incident Management Policy

Managing Government Information Policy

Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia

7. DEFINITIONS/GLOSSARY

The following key words in this document are to be interpreted as described in RFC 2119 (see https://tools.ietf.org/html/rfc2119): MAY; MUST; MUST NOT; OPTIONAL; RECOMMENDED; REQUIRED; SHALL NOT; SHALL; SHOULD; and, SHOULD NOT.

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revision
1.0	2019-09-30	Daniel Surdu	New
2.0	2021-10-07	Kristina Petrosyan	New template. Reordered and updated content, definitions for IT Assets and requirements for asset inventory. Guidelines created to provide clarification on standard.

9. CONTACTS

For questions or comments regarding this standard, please contact:
ISB Branch, OCIO
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca