Document Version: 1.0
Effective Date: December 15, 2021

Asset Management Security Guidelines

Contents

1 Introduction

Information and information systems constitute valuable government resources that are critical to the efficient and secure delivery of government services. Everyone plays a role in securing and protecting the information and technology assets required to deliver those services. Securing IT Assets means knowing what assets you have,the classification of those assets, who is responsible for them, and where they are located. The Asset Management Security Standard establishes baseline security controls that implement the government's Defensible Security Principles for the protection of government confidential information and the physical IT assets used to deliver services.

1.1 Document Purpose

These guidelines help clarify and support the Asset Management Security Standard. They provide support to the ministries in order to implement best practice IT and information asset management processes and to comply with the Asset Management Security Standard.

Guidelines are intended for ministry resources who are responsible for:

- Requesting IT Assets;
- Approving and procuring IT Assets;
- Maintaining inventories of IT Assets; and
- Ensuring compliance with government IM/IT and procurement and IT asset management policies and standards.

These guidelines describe OCIO inventory responsibilities for the IT Assets provided to ministries, and ministry responsibilities to inventory the IT Assets they acquire from vendors. Detailed information describes OCIO and ministry roles and responsibilities (see Asset Inventory Responsibilities section), as well as ministry processes and compliance activities (see your ministry's IT AM Process documentation for ministry-specific details).

An overview of inventory management processes for each stage of the asset lifecycle describes how to add and update inventory information. It applies to physical IT assets, information assets, and software or cloud asset inventory requirements.

2 What to Inventory?

2.1 IT Asset Definition & Scope

According to the Core Policy and Procedures Manual (CPPM) Chapter 8: Asset Management and CPPM Chapter I: Tangible Capital Assets, an IT Asset is a tangible asset that costs $10,000 or more. It can also be a non-capitalized/expendable asset that contains or stores unencrypted sensitive data. To simplify, IT Asset Owners must maintain an IT Asset inventory for IT Assets that meet one or more of the following criteria:

- Contains or stores unencrypted sensitive data classified as Confidential according to the Information Security Classification Standard;
- Can be remotely exploitable and used to gain unauthorized access to government networks; or,
- Costs $10,000 or more.

2.2 Physical Asset Definition & Scope

An IT Asset is any software or hardware component of an IT product or service. A **physical IT asset** is a hardware device such as:

- End-user devices: workstations, laptops, tablets, smartphones, and SIM cards;
- Network and telecommunication equipment: routers, switches, load balancers, and video-conferencing and voice over Internet protocol (VoIP) systems;
- Data center infrastructure hardware: servers, storage and backup systems, utilities, and security equipment;
- Peripheral devices: personal printers, monitors, scanners, multifunction printing systems;
- Internet of Things devices: Smart TVs, network connected video cameras; and
- Line of Business (LoB) devices: avalanche sensors and traffic light controllers.

In Scope Physical IT Assets

Physical IT assets that expose government information and/or the government network to cybersecurity vulnerabilities need to be inventoried and protected. Inventory requirements consider the IT Asset's vulnerabilities and risk position.

1. Vulnerabilities

⇒ Connectivity

- Is the device connected or can it connect to the government network and/or the internet?
- Is it remotely exploitable?
- Could it be used to gain unauthorized access to BC Government networks?

⇒ Security

- Is the device portable or in a secure location? Portable devices that are easily lost or stolen, such as laptops and mobile phones need to be inventoried.

- Does it have an administrator and secure password? Smart TVs with Wi-Fi capability that are not password protected are vulnerable.

⇒ Encryption

- Is the device fully encrypted? Portable hard drives and USB/thumb drives that are obtained from the OCIO and are fully encrypted do not need to be inventoried. Unencrypted storage devices are forbidden.

2. Risk Position

⇒ Threat/attack impact

- Does the device contain data classified as sensitive or confidential?
- Is the asset part of a government mission critical system?
- Is the asset expensive to replace (i.e., >$10,000)?

⇒ Threat/attack likelihood

- Does the device have built-in protection or is it monitored by the OCIO or a ministry security team?
- How likely is it that an employee error could result in an information incident or privacy breach? Is the asset or whatever it's connected to attractive to bad actors? Remember, just because it hasn't happened yet, doesn't mean it can't happen.

2.3 Information Asset Definition & Scope

According to the Managing Government Information Policy, information is "any collection of data that is processed, analyzed, interpreted, classified or communicated in order to serve a useful purpose, present fact, or represent knowledge in any medium or form." An **information asset** is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognizable and manageble value, risk, content, and lifecycle. Information assets include:

- Software and services, including computer and communications services and general utilities;
- Cloud services and information, and data assets in the cloud;
- 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 valuable information assets including database and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, and archived information.

In Scope Information Assets

Information assets that serve a useful purpose, present fact, or represent knowledge in any medium or form, that may have financial value and/or are essential in providing a service or in decision-making, need to be protected and inventoried.

2.4 IT Asset Categories and required inventory fields

2.4.1 IT Asset Attributes

IT Asset inventories exist to provide asset information in situations such as information security incidents and investigations, servicing, license renewals, end-of-life replacement planning, etc. Specific attribute requirements depend on the asset category. Mandatory attribute types specify the minimum information required to satisfy the objective.

Mandatory Attribute Type & Objective	Examples
Identification attributes provide a unique IT Asset identifier.	• In addition to its Name, Category/type, Manufacturer, Model and Version, the inventory record requires an Asset Number, Serial number, IP or MAC address to distinguish it from other assets of the same type, manufacturer, model/version.
Ownership attributes enable the IT Asset to be located and retrieved.	• Individually assigned assets need a minimum of employee name, organization, location, and phone and email contact information. • IT Assets owned by an organization (e.g., Service Desk) need a minimum of Organization name, location, and contact number or email.
Asset management attributes indicate the IT Asset's operational status.	• Is the IT Asset commissioned/in service or decommissioned/not in service? What are the corresponding dates when the operational status changed? If the asset can't be accounted for, has it been reported as lost or disposed of? • Other attributes may support repair and warranty inquiries: Vendor/provider; Licence information; Backup information and location; end-of-life date.
IT Asset risk attributes indicate the level of security the asset requires.	• Depending on the IT Asset category, risk attributes could include: ○ Security classification; ○ Network security zone; ○ Sensitivity and safeguard requirements; ○ Criticality for service delivery and maintaining business functions; ○ Consequences of loss; and, ○ Other relevant risk information.

2.4.2 IT Asset Categories

The OCIO has identified the following IT Asset categories as vulnerable and requires them to be inventoried. The following lists the minimum required attributes for each asset category (and if an organisation wants to track more they can):

IT Asset Category	Identification Attributes	Ownership / Responsibility Attributes	Management Attributes	Risk Attributes
Workstations	• Asset tag number – to uniquely identify the asset • Make and model – to determine vendor support • Serial number – identifies manufacturer unique number	• Person assigned – name and contact information	• Asset provider • Commission date • Status	• Encryption status
Mobile devices (including tablets)	• Asset tag number – to uniquely identify the asset • Make and model – to determine vendor support • Serial number – identifies manufacturer unique number	• Person assigned – name and contact information	• Asset provider • Commission date • Status	• Encryption status
Infrastructure (infrastructure servers, DNS, DCs), network and printing devices	• Asset tag number – to uniquely identify the asset • Make and model – to determine vendor support • Serial number – identifies manufacturer unique number	• Branch or department responsible • Contact information	• Asset provider • Commission date • Status • Support organisation	• Data classification • Criticality
IoT and telecommunication devices	• Asset tag number – to uniquely identify the asset • Make and model – to determine vendor support • Serial number – identifies manufacturer unique number	• Branch or department responsible • Contact information	• Asset provider • Commission date • Status • Support organisation	• Criticality
Information assets and servers (LoB applications, databases, systems)	• Asset tag number – to uniquely identify the asset • Make and model – to determine vendor support	• Branch or department responsible • Contact information	• Asset provider • Commission date • Status • Support organisation	• Encryption status • Data classification • Criticality

2.5 Exceptions: Excluding Low & No Risk IT Assets

Ministries can exclude low and no risk IT Assets as follows:

IT Asset Risk Level	Description	Exclusion Requirements
No risk	• Fully encrypted, and/or • Permanently hardened against internet use, and/or	The device's disabled status can be tracked.

IT Asset Risk Level	Description	Exclusion Requirements
	• Data network connectivity disabled (its ethernet port is physically disabled, Bluetooth and Wi-Fi connectivity are permanently set to OFF/disabled), and/or • Administrator access for the device is password protected and was changed from the factory default.	
Low risk	• Connected or capable of connecting to a data network/the internet, and/or • Protected/secure access, and/or • Fully encrypted.	Complete a risk assessment such as a STRA and document the findings (e.g., *Statement of Acceptable Risk* form) to justify the exclusion.
Medium risk devices	• Connected or capable of connecting to a data network/the internet, and/or • Protected/secure access, and/or • Partly encrypted.	No exclusions – inventory is mandatory.
High risk devices	• Connected or capable of connecting to a data network/the internet, and/or • No protected/secure access, and/or • Not encrypted.	No exclusions – inventory is mandatory.

3 Asset Inventory Responsibilities

3.1 OCIO Inventory Responsibilities

OCIO is responsible for managing asset inventories for the devices they provide to ministries. Ministries normally acquire the following physical IT Assets using OCIO services:

- Workstations/laptops;
- MPS Printers;
- VOIP phones (UC accounts);
- MTR and Skype conferencing devices (with UC accounts); and
- Infrastructure devices.

3.2 Ministry Inventory Responsibilities

Ministries are responsible for keeping the OCIO informed/updated on assignee information and device status (lost, stolen, damaged or disposed of) related to OCIO provided devices. Ministries are also responsible for managing asset inventories for all IT and information assets that are not acquired from the OCIO:

- Workstations/laptops not provided by the OCIO (i.e., procured directly from a vendor or provided by a third party);
- Non-MPS printers acquired from a vendor or service provider;
- Conferencing devices not provided by the OCIO (that are network connected and do not have a Unified Communications (UC) account);
- Infrastructure devices not provided by the OCIO;
- Mobile devices (mobile/smart phones and tablets);
- Internet of Things devices, including Smart TVs (any device with data network/internet connectivity capability, whether or not it is connected); and
- LoB devices and systems that meet the definition of an IT Asset and must be inventoried based on risk assessment.

4 AM Roles & Responsibilities

IT and information asset inventory information must be available to the security resources responsible for protecting those assets. The OCIO maintains inventories of the IT Assets it provides to ministries; ministries are responsible for allocating resources and establishing processes to maintain inventories of IT and information assets not acquired from the OCIO. Ministries are also responsible for allocating resources and establishing processes for the handling of IT and information assets in their ministries.

4.1 AM Governance

OCIO Governance Roles	Responsibilities
Government Chief Information Officer (GCIO)	• Establishes and ensures ministry compliance with corporate-wide Information Security Policy, IM/IT standards, including the AM Security Standard.
Chief Information Security Officer (CISO)	• Communicates government AM Security Standard requirements and provides implementation guidelines to ministries; and • Establishes processes to assess AM Security Standard compliance.

Ministry Governance Roles	Responsibilities
Ministry Chief Information Officer (MCIO)	• Communicates government AM Security Standard requirements to ministry stakeholders; • Allocates resources to develop, implement, and maintain ministry IT and information asset procurement and inventory management and asset handling policies and processes; and, • Accountable to the GCIO for AM process compliance.
ADM, Executive Director, IT Director,	• Develops, implements, and maintains ministry IT and information asset procurement and inventory management and asset handling policies and processes; and, • Establishes AM compliance reporting processes.

Ministry Information Security Officer (MISO)	• Uses IT Asset inventory information (e.g., asset owner/assignee, location, operational status) to investigate an IT physical asset in question (where applicable) and information security incidents; and, • Conducts risk assessments to determine if IT Assets that do not belong to a mandatory inventory category need to be inventoried (i.e., are above or below the ministry's risk threshold).

4.2 Ministry IT Asset Procurement Process

Roles	Responsibilities
Requestor *(Requestor cannot be the Approver)*	• Identifies the appropriate ministry procurement and approval process for the asset category; • Completes the request and submits it for approval; and • Ensures that supervisors submitting requests for new employees provide asset inventory information, including assigning the IT Asset to the new employee on the start date.
Approver (Expense Authority) *Approver cannot be the Requestor*	• Ensures the following prior to approval: ○ If no inventory already exists for the requested IT Asset, contacts the MISO to initiate a risk assessment to determine if the asset must be inventoried; ○ If an inventory already exists, notify the Inventory Owner and provide asset attribute information; ○ If the IT Asset is to be excluded from the inventory because it is considered low or no risk, note the risk assessment document number on the request. • Works with the MISO and MCIO to request resources when new inventories must be established; and, • Provides financial approval for the request only when inventory responsibility for the asset is known and Inventory Owner resources have been allocated.
Purchaser	• Receives the approved request; and • Purchases the asset from the vendor and arranges receipt and delivery to the requestor.

4.3 Ministry AM Process

Role	Responsibilities
Asset Assignee/Owner	• An individual employee (for personally assigned IT assets such as workstations and mobile devices) or an organization (for group-owned devices such as the Service Desk for branch owned Smart TVs or plotters); • Responsible for security of the IT or information asset (Appropriate Use Policy), including ensuring that asset is inventoried, and that inventory information is correct;

	• Uses the ministry process to document, approve, and submit change requests to the Inventory Owner to update asset information (e.g., change to assignee, location, operational status); • Locates or confirms asset location in an incident situation; • Reports missing or damaged assets (GILR and/or Information Incident Process); and • Uses the government Asset Inventory Recovery (AIR) process to dispose of damaged or end-of-life physical IT assets or sends it to the delegated ministry resource to manage the disposal process.
Asset Assignee Supervisor	• Recovers assigned IT and/or information assets from terminated employees; and, • Submits change requests to the Inventory Owner to update IT or information asset status, assignment, and/or when an asset's key attributes have changed (e.g. IT asset re-assigned).
Inventory Owner	• Receives notification of approved or requested IT or information asset, including new asset attribute information; • Creates a new inventory record; adds new IT or information asset attributes; verifies accuracy; • Receives approved change requests, updates the inventory records, and verifies accuracy; • Conducts ongoing operational reviews of inventory records; checks accuracy and completeness; investigates errors and missing information; requests approval for corrections; processes updates; • Reports missing assets (GILR and/or Information Incident Process); • Processes requests to decommission and disposal of IT assets (as authorized) or forwards disposal requests to the MISO for approval; • Closes inventory records for IT assets sent to AIR; and • Ensures access/updates to asset inventory records are logged and that there is security for the inventory records and access logs.

4.4 AM Compliance Review Process

Role	Responsibilities
Inventory Owner	• Supports the compliance review process; provides inventory reports or inventory access to the assigned reviewer; and, • Verifies and processes corrections identified by the operational or compliance review of the inventory.
Inventory Reviewer *(when feasible, should not be the Inventory Owner)*	• Spot-checks inventory reports and/or records; • Confirms that change requests are processed promptly; and • Confirms that access to inventory records is secure and is logged.
Compliance Evidence Owner	• Schedules and manages the ministry's AM inventory review(s); and • Maintains correspondence from inventory reviewers confirming inventory review completion.

MCIO	• Reports AM compliance to the GCIO.

5 AM Best Practices

5.1 Secure Inventory Access

Access to IT and information asset inventories should be limited to authorised personnel. Access and changes to inventory records should be logged.

5.2 Asset Inventory Lifecycle

AM best practices ensure that IT and information assets are tracked through each stage of the asset's lifecycle:

- **Planning** for new assets means ensuring that inventories and inventory management processes exist, and that Inventory Owners are informed of new assets;
- **Procuring** assets means adding asset information to the inventory;
- **Deploying** assets means updating inventory information to reflect deployed, or in service status;
- **Managing** assets means keeping track of assets and updating asset information; and
- **Retiring** and disposing of assets means using appropriate disposal processes and updating the inventory when assets are no longer in service.

5.2.1 Planning for new assets

Planning ensures that an Inventory Owner has been identified or assigned and that an inventory exists or will be created to manage the requested asset. The planning process should include a process to inform the Inventory Owner of the new asset and provide the required asset attribute information. Requests should not be approved until inventory requirements are met.

See How to Exclude Low and No risk assets from inventory.

5.2.2 Procuring assets and creating inventory records

IT Asset procurement is subject to government Core Policies and Procedures and IM/IT procurement policies.

Ministries can avoid inventory ownership responsibilities by procuring IT assets using established OCIO services to request:

- Workstations;
- MPS Printers;
- Conferencing Devices;
- Infrastructure Devices; and,
- Cloud Services.

Ministries that procure IT and information assets directly from a vendor or third party require Inventory Owners, and inventory tools and processs to manage inventories of those assets. Examples:

- All ministries that procure mobile phones directly from approved vendors. Ministries are responsible for ensuring that the resources who order mobile phones understand their role in tracking them from order through disposal;
- Ministries with workstations obtained directly from a vendor or a third party MUST maintain an inventory of those workstations and establish processes that inform the Inventory Owner when a workstation needs to be added, changed, removed from service, or disposed of;
- Ministries that purchase non-MPS printers MUST maintain an inventory of those devices and establish processes to ensure that the Inventory Owner is notified when a non-MPS printer is being added, changed, removed from service or disposed of; and,
- Ministries that purchase cloud-based assets directly from a cloud service provider MUST maintain an inventory of those cloud-based assets and establish processes to ensure that the resources who procure cloud-based assets understand their role in tracking them from procurement through retirement/decommission.

5.2.3 Deploying assets and updating inventory information

Ministries are responsible for establishing processes to ensure that when an IT or information asset is deployed, assigned to a user/owner, or commissioned into service, that the Inventory Owner is informed and that the inventory record is updated to reflect the change in asset status, ownership/assignment, location, etc.

5.2.4 Managing and tracking assets

Ministries are responsible for establishing processes to ensure that asset assignees/owners or their supervisors inform Inventory Owners of changes to asset information resulting from reassignment, termination, replacement, repair, upgrades, moves, etc. Supervisors should verify that assets returned by a terminating employee match the asset's inventory records. Supervisors should also ensure that the control over cloud-based assets that were procured and controlled by a terminating employee is reassigned.

In addition to a formal documented review (at least annually), Inventory Owners should conduct regular operational reviews to track assets and ensure that inventory information is complete and accurate.

☞ Note: Ministries are responsible for using the appropriate OCIO process to ensure that OCIO inventory information is kept current. See the appropriate AM Procedure document for details.

5.2.4.1 Report lost or stolen asset

When an asset is lost or stolen the owner or assignee completes a General Incident or Loss Report (GILR) and informs the Inventory Owner.
Where the loss, theft or misappropriation involves information, the owner or assignee MUST also follow Information Incident Management Process.

The Inventory Owner updates the inventory to reflect the asset's status as decommissioned/out of service.

5.2.5 Retiring and disposing of assets

When an IT asset is irrepairable or at end of life, it MUST be disposed of securely and in accordance with the government asset disposal process. When an information asset is at end of life, it MUST be disposed of securely and in accordance with the Managing Government Information Policy. The asset owner/assignee informs the Inventory Owner who updates the inventory. Consult the Ministry Records Officer prior to disposing of IT assets that were used to store government records.

6 Asset Information Classification

6.1 Asset Information Labelling Procedures

Information labelling communicates the information security classification and protection requirements to employees. Ministries MUST document procedures to label IT and information assets with their appropriate information security classification in accordance with the Information Security Classification Standard.

Information types that MUST be considered for labelling include: printed or electronic records, reports, files, on-screen displays or messages. Ministries MUST select and document the appropriate label type for each information type.

Automatic information labelling MUST be used where possible (e.g. document templates, standard report footers, printer watermarks, on-screen displays, or system-applied text).

Where direct information labelling is not possible, alternate methods MUST be used to communicate the information security classification, such as marking of storage media used, a description in information sharing agreements, system interface specifications or use of metadata.

7 Asset Handling

7.1 Asset Handling Procedures

Ministries MUST document asset handling procedures appropriate for information security classification and criticality of the IT or information asset for secure processing, storage, transmission, declassification and disposal.

Procedures MUST also be defined for interpreting the information security classification labels from, and handling information exchanged with, other jurisdictions.

When dealing with IT or information assets, the following MUST be considered:

- Access restrictions that support the protection requirements appropriate to the information security classification and criticality of the asset;
- Protection of temporary or permanent copies of the information asset - the protection MUST be consistent with original copy of the information asset;
- Storage of IT assets in accordance with manufacturers' specifications; and,
- Clear marking of all copies of media used to store or contain the information asset for attention of the authorized recipient.

Information sharing agreements MUST include:

- Procedures to identify the information security classification of that information;
- Interpretation of the classification labels from other organizations; and,
- Level of protection required for the information.

7.1.1 Media Handling Procedures

Ministries MUST document media handling procedures that are compliant with the information security classification and handling requirements for information stored on the media. If information of various information security classification levels is stored on the media, the media MUST be handled according to the highest information security classification level of the information stored.

Only approved media devices appropriate for the information security classification and criticality of the information being stored MUST be used.

Media handling documentation MUST include procedures for:

- Marking of media with its highest information security classification level label that indicates the sensitivity of the information contained on the media;
- Access control restrictions and authorization for the media handling based on the information security classification label;
- Correct use of technology (e.g. encryption) to restrict and enforce access control appropriate to the information security classification label used;
- Copying and distribution of media, including minimization of multiple copies, marking of originals and distribution of copies;
- Operating the media storage environment and managing media lifespan according to manufacturer specifications;
- Regular status accounting of media;
- Maintenance of media transfer and storage records;
- Media destruction and disposal; and,
- Employee training on the protection of the media.

7.1.2 Media Transport Requirements

Minimum transport requirements for physical media used to store information are:

- Use of couriers that are approved by government;
- Inspection of identification credentials of couriers upon pickup and delivery of media;
- Obtainment and retention of receipts for media shipments;

- Use of packaging that will protect the media from loss or damage; and,
- Use of packaging that will obscure the information security classification label on the media.

8 Supporting documents

This document supplements the Asset Management Security Standard. The AM Security Standard is a sub-section of and is designed to be read in conjunction with the Information Security Standard (version 2.0). See: IM/IT Standards.

Core Policy and Procedures Manual:

- Chapter 6: Procurement
- Chapter 8: Asset Management
- Chapter 12: Information Management and Information Technology Management; and
- Chapter 15: Security

Managing Government Information Policy
Information Security Standard (version 2.0)
Information Security Classification Standard
Information Security Classification Guidelines
Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia

Procedure documents *(coming soon)*

Related Defensible Security Elements

Asset management

9 Revision History

Version	Revision Date	Author	Description of Revision
1.0	2021-10-07	Kristina Petrosyan	New

10 Contacts

For questions or comments regarding this document, please contact:

Information Security Branch, OCIO
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca