ASSET MANAGEMENT SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0
Published: September 2019
### Table of Contents

I  INTRODUCTION, SCOPE, BACKGROUND ........................................................................................................3

II  GLOSSARY, TERMS AND DEFINITIONS, LIST OF COMMONLY USED REFERENCES ........................................3

1  ASSET MANAGEMENT .........................................................................................................................................4

  1.1 RESPONSIBILITY FOR ASSETS ....................................................................................................................4

  1.2 INFORMATION CLASSIFICATION ..................................................................................................................7

  1.3 REMOVABLE MEDIA .....................................................................................................................................11
I  Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II  Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references” sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.
1 Asset Management

Information and information systems services constitute valuable government resources. The asset management chapter establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

To account for the assets that require protection, this chapter specifies the requirement to designate who owns assets. Designated owners become responsible for protecting information and technology assets and to maintain the way assets are protected.

This chapter sets the foundation for a system that classifies information to identify different security levels, to specify how much protection is expected and how information should be handled at each level. Not all information requires the same level of protection because only some information is sensitive or confidential.

1.1 Responsibility for assets

1.1.1 An inventory of all important assets associated with information systems must be documented and maintained.
   a) Identification of assets
   b) Documenting and maintaining asset inventories
   c) Loss, theft or misappropriation of assets

Purpose: To identify organizational information assets and define appropriate protection responsibilities.

1.1.1 a) Identification of assets
Information Owners must identify assets under their control including:
   • Software;
   • Hardware including mobile devices and tablets;
   • Services including computer and communications services and general utilities;
   • 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 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.

1.1.1 b) Documenting and maintaining asset inventories
Information Owners and Information Custodians must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of an enterprise risk management strategy.

Information Owners and Information Custodians must document, maintain and verify the personal information directory including the personal information bank and privacy impact assessment sections.
The following information should be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss, disposal or destruction:

- Type of asset;
- Ownership;
- Format;
- Location;
- Back-up information and location;
- Licence information;
- Sensitivity and safeguards requirements;
- Criticality for service delivery and maintaining business functions; and,
- Consequences of loss.

Information Owners and Information Custodians are accountable for asset identification and inventory maintenance.

1.1.1 c) Loss, theft or misappropriation of assets

The loss, theft or misappropriation of assets must be reported immediately using the General Incident or Loss Report. Where the loss, theft or misappropriation involves information, the Information Incident Management Process must be followed.

**Recommended Tests:**

*Note: 1.1.1 is reported on as part of the annual information security review.*

- Demonstrate that assets are identified and tracked throughout the asset's life-cycle, i.e., creation, processing, storage, transmission, deletion, and disposal.
- Demonstrate the inventory of information assets is regularly inspected for correctness.
- Demonstrate information assets are properly classified and the criticality of the asset is identified.
- Demonstrate Executive support in asset management.
- Demonstrate information incidents and loss of assets are reported immediately.

1.1.2 Information Owners and Information Custodians must be designated for all assets associated with information systems.

*Purpose:* To designate custodians for assets, with approved management responsibility, for the protection of organizational assets associated with information and technology systems or services.

1.1.2 a) Responsibilities for asset ownership

All information assets must have a designated owner.

An Information Owner is responsible for controlling the production, development, maintenance, use and security of information and technology assets within their jurisdiction. Information Owners are responsible for:

- Ensuring the appropriate classification and safeguarding of information and technology systems or services;
• Defining and regularly reviewing access restrictions, classifications and safeguards in accordance with applicable policies; and,
• Designating Information Custodians and ensuring that they have the correct tools for protecting designated assets.

1.1.2 b) Designating Information Custodians
Information Owners may delegate responsibility for custody of information and technology systems or services to Information Custodians.

Information Custodians will be responsible for:
• Overseeing the functioning of information and technology assets;
• Delivery of services in accordance with defined service requirements; and,
• Regular reporting on designated information and technology assets.

Guidelines:
Ownership and custodianship responsibilities should be defined and monitored within the employee’s Performance Management tool “MyPerformance Profile”.

Recommended Tests:
Note: 1.1.2 is reported on as part of the annual information security review.
• Demonstrate that ownership is reflected in the information assets inventory.
• Demonstrate owners have considered access restrictions, classification, safeguards and handling for information assets.
• Demonstrate regular reporting status of information assets to the owner.
• Demonstrate ownership in security reviews (e.g., Security Threat and Risk Assessments, Privacy Impact Assessments).

1.1.3 Rules for the acceptable use of information systems must be identified, documented and implemented.
a) Acceptable use of government resources

Purpose: To prevent misuse or compromise of government information systems.

1.1.3 a) Acceptable use of government resources
All users of government information systems must take responsibility for, and accept the duty to actively protect, government information and technology assets.

The requirements and terms of use of government information systems, including personal use, are described in CPPM Section 12.3.1 - Appropriate Use of Government Information and Information Technology Resources (Appropriate Use Policy).

Recommended Tests:
Note: 1.1.3 is reported on as part of the annual information security review.
• Demonstrate employees accessing information assets are aware of the Appropriate Use Policy.
• Demonstrate supervisors authorize the downloading of applications and software.
• Demonstrate employees are familiar with the responsibilities for information asset loss reporting.
1.1.4 Employees must return government assets upon termination or change of employment.  

a) Return of assets

**Purpose:** To ensure employees return physical and information assets at termination or change of employment.

1.1.4 a) Return of assets
Supervisors must document the return of government assets in the possession of employees upon termination of their employment using standard processes. These processes must ensure the:

- Return of:
  - documents, files, data, books and manuals in physical or other media formats including other information assets developed or prepared by an employee or contractor in the course of their duties,
  - computer hardware, software and equipment (e.g., mobile devices, portable media), and,
  - access devices, cards, vouchers and keys (e.g., credit cards, taxi cards, travel vouchers);
- Returned items are verified against established asset inventories;
- Recovery or compensation for assets not returned, based on established criteria regarding depreciation and replacement value for classes of items; and,
- Identification of unreturned access devices, cards and keys that could permit unauthorized access or alteration, disposal or destruction of assets, so that information and security systems can be protected.

**Recommended Tests:**

*Note: 1.1.4 is reported on as part of the annual information security review.*

- Demonstrate the information asset inventory is reviewed for all assets on loan at termination.
- Demonstrate a formal procedure to recover information assets at termination, including document files, electronic storage devices, computers, mobile devices, access cards and/or keys.

1.2 Information classification

1.2.1 The government information security classification system must take into account the value, sensitivity and intended use of the information.

**a) Information and information system security classification**

**b) Mandatory features of information security classification**

**c) Mandatory features of information system security classification**

**Purpose:** To define the information security classification system characteristics for information and information systems.

1.2.1 a) Information and information system security classification
Information Owners and Information Custodians must use the Information Security Classification system to categorize information and information systems.

The Office of the Government Chief Information Officer is responsible for definition, application and enforcement of the Information Security Classification system.
Risk Management Branch and Government Security Office are responsible for definition of Security Categories.

**1.2.1 b) Mandatory features of information security classification**

The Information Security Classification system must:

- Apply to information types rather than discrete data elements;
- Determine the relative value of information including factors such as:
  - Statutory or regulatory requirements,
  - Impact to health, life or personal safety,
  - Effects of data aggregation,
  - Impact to the Ministry service plan from loss of information confidentiality, integrity and availability, and,
  - Changes to information sensitivity over time;
- Maintain compatibility with the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS).

The Information Security Classification system must include processes for:

- Defining information types for categorization;
- Making decisions on categorization of information; and,
- Periodic reassessment of the information security categorization processes.

**1.2.1 c) Mandatory features of information system security classification**

The Information Security Classification system must include processes for:

- Categorization of information systems based on the security classification of information stored, handled or processed by the information system; and,
- Inclusion of information and system security classification documentation in the System Security Plan.

**Guidelines:**

The Information Security Classification system is a cornerstone of security and risk assessment activities. The security categories communicate the value and classification of information in a way that allows for decisions to be made about risk management and information handling.

Information Security Classifications assist in:

- Consistent, comparable Statement of Sensitivity descriptions of the Security Threat and Risk Assessment describing the confidentiality, integrity and availability requirements of the assessed system.
- The selection of system security controls - service providers can bundle system security controls into packages or service offerings based on the consistently defined protection requirements of the information.
- The selection of, and consistent application of, information handling and labeling rules.
- Information sharing agreements by indicating the relative value of information being exchanged in a consistent and comparable manner across government.

**Recommended Tests:**

*Note: 1.2.1 is reported on as part of the annual information security review.*
- Demonstrate that information applications and information technology have Security Threat and Risk Assessments completed that consider information classification.
- Demonstrate that personal information has a Privacy Impact Assessment conducted.
- Demonstrate that classified information is processed, handled, stored and transmitted according to information classification sensitivity.
- Demonstrate that an injury or harm test is completed on information to determine proper classification.
- Demonstrate that information security classification is applied across the Ministry.

1.2.2  Information must be identified, labelled when appropriate and handled in accordance with the assigned information security classification.

   a) Information labelling procedures
   b) Information handling procedures

Purpose: To protect information in accordance with its security classification.

1.2.2 a) Information labelling procedures
Information Owners and Information Custodians must document procedures to label information with its information security classification as required by the government Information Security Classification system. Information labelling communicates the security classification and protection requirements to employees.

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

Automatic information labelling must be used where possible (e.g., by use of 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 storage media, a description in information sharing agreements or system interface specifications or use of metadata.

1.2.2 b) Information handling procedures
Information Owners and Information Custodians must document information handling procedures for secure processing, storage, transmission, declassification and disposal of information assets.

Information protection procedures must take into account the information security classification, labelling and handling processes and the access control policies.

Guidelines:
During systems development, specify the information security labelling requirements when defining business requirements for reports, screens and data storage.
Recommended Tests:

Note: 1.2.2 is reported on as part of the annual information security review.

- Demonstrate information in all formats is labeled in accordance with its sensitivity.
- Demonstrate all media formats can be marked with appropriate sensitivity labels.
- Demonstrate labeling is automated with the use of templated documents when appropriate.

1.2.3 Information assets must be handled and stored so as to prevent unauthorized information disclosure or misuse, in accordance with the information security classification system.

a) Asset handling procedures
b) Media handling procedures

Purpose: To ensure that documented procedures are used for handling information assets and storage of media in accordance with the security classification of information stored on the media.

1.2.3 a) Asset handling procedures

Information Owners and Information Custodians must follow the procedures for information security classification when handling information assets.

The following items must be considered when dealing with information assets:

- Access restrictions supporting the protection requirements for each level of classification;
- Protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
- Storage of IT assets in accordance with manufacturers’ specifications; and,
- Clear marking of all copies of media for the attention of the authorized recipient.

Information sharing agreements must include:

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

1.2.3 b) Media handling procedures

Information Owners and Information Custodians 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 security classifications is stored on media, the media must be handled according to the highest classification of the information stored.

Media handling documentation must include procedures for:

- Marking of media to its highest information classification level label, in order to indicate the sensitivity of information contained on the media;
- Access control restrictions and authorization;
- Correct use of technology (e.g., encryption) to enforce access control;
- 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.

Only approved media devices appropriate for the classification of the information being stored must be used.

**Recommended Tests:**

*Note: 1.2.3 is reported on as part of the annual information security review.*

- Demonstrate access restrictions support the classification of assets.
- Demonstrate procedures are in place for storage of classified assets commensurate with the sensitivity label.
- Demonstrate transmission considerations are based on classification (e.g., highly sensitive material is not placed in the mail but sent via bonded courier).

### 1.3 Removable media

<table>
<thead>
<tr>
<th>1.3.1</th>
<th>All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Management of government records</td>
</tr>
<tr>
<td>b)</td>
<td>Use of portable storage devices</td>
</tr>
<tr>
<td>c)</td>
<td>Human factors</td>
</tr>
<tr>
<td>d)</td>
<td>Risk assessment factors and controls</td>
</tr>
<tr>
<td>e)</td>
<td>Mandatory controls</td>
</tr>
</tbody>
</table>

**Purpose:** To ensure that risks to information introduced by portable storage devices are managed.

#### 1.3.1 a) Management of government records

Corporate Information and Records Management Office is responsible for the management and disposal of government records according to records schedules approved under the Information Management Act.

#### 1.3.1 b) Use of mobile or portable storage devices

The use of mobile or portable storage devices to store or transport information increases the risk of information compromise. These devices are typically small, and are easily lost, stolen or damaged, particularly when transported in public environments. Mobile or portable storage devices include, but are not limited to, USB drives, external hard drives, smartphones, tablets, laptops, and mp3 players.

Information Owners, Information Custodians and Supervisors must:

- Ensure that use of mobile or portable storage devices is managed and controlled to mitigate risks;
- Document processes for authorizing use of mobile or portable storage devices; and,
- Ensure employees using mobile or portable storage devices protect information and information technology assets in their custody or control.
Information Owners or Information Custodians must conduct a Security Threat and Risk Assessment on mobile devices or mobile computing services to determine the risk profile and suitability of the device or the service for government use prior to deployment within government.

Technical standards for each device type must be documented including product name, mandatory controls, permitted information classifications and strength of controls such as encryption key length. Device handling procedures should include instructions to minimize the amount of information stored on mobile or portable storage devices.

1.3.1 c) Human factors
Information Owners, Information Custodians and Supervisors must ensure employees using portable storage devices are:
- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with the required protection technologies and when they must be used; and,
- Familiar with the Information Incident Management Process and General Incident or Loss Reporting procedures.

1.3.1 d) Risk assessment factors
The Security Threat and Risk Assessment must consider the impact of disclosure or loss of information stored on portable media from threats such as:
- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media disposal or destruction;
- Improper long-term storage environment;
- Exposure to malware; and,
- Incomplete erasure of data prior to device disposal.

Information classification and sensitivity levels must be considered in the risk assessment.

1.3.1 e) Mandatory controls
Minimum information protection safeguards for the use of portable storage devices must include:
- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Documented definition of information classifications or sensitivities permitted to exist on specific media types;
- Not storing the only version of a document on portable storage devices;
- Documented authorization processes for use of portable storage devices;
- Encryption of stored data;
- Contractual requirements for external parties that transport, handle or store portable storage devices; and,
- Adherence to manufacturer specifications for use of portable storage devices.

Documented portable storage devices handling procedures include:
- Off-site storage;
- Third party transportation;
- Information backup;
- Protection against malware;
• Logging of media custody and location to allow for accounting and audit;
• Media labelling to indicate owner, classification and special handling restrictions;
• Maintenance of information where the information storage requirement exceeds the expected media lifetime; and,
• Secure erasure and disposal.

Recommended Tests:

**Note:** 1.3.1 is reported on as part of the annual information security review.

- Demonstrate portable storage devices are stored commensurate with the classification of the information they contain.
- Demonstrate that cryptographic controls are applied for sensitive material storage.
- Demonstrate that procedures are in place to scan portable storage devices for malware.

<table>
<thead>
<tr>
<th>1.3.2</th>
<th>Media must be disposed of securely and in a manner appropriate for the sensitivity of the data it contains.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Secure disposal and destruction of media</td>
</tr>
</tbody>
</table>

**Purpose:** To ensure that information cannot be retrieved from media that is no longer in use.

**1.3.2 a) Secure disposal and destruction of media**

Any asset capable of storing electronic information is considered a type of media, including mobile and portable storage devices, hard disks, CDs, DVDs, and tapes. Information Owners and Information Custodians must ensure that media that is no longer required operationally (e.g., due to expiry, surplus, damage or wear) is disposed of securely. Prior to disposal, the Ministry Records Officer must be consulted.

Media disposal procedures must:

- Be documented and communicated to employees;
- Specify erasure and disposal measures whose strength is based on information sensitivity and type of media (e.g., erasure software);
- Include secure disposal or destruction of media if erasure is not sufficient, or not cost effective (e.g., destruction by shredding, incineration or chemical dissolution);
- Include secure storage measures for media collected for and awaiting erasure or disposal, to avoid undetected theft of small amounts of media from large volumes awaiting disposal; and,
- Include audit logs of media disposal.

Corporate Information and Records Management Office is responsible for ensuring secure disposal services are available to Information Owners and Information Custodians.

**Guidelines:**

A Corporate Supply Arrangement exists for provision of secure media disposal services. Secure disposal service companies should be used where practical to perform media disposal. Contact the Ministry Records Officer for further details.

**Recommended Tests:**

**Note:** 1.3.2 is reported on as part of the annual information security review.
• Demonstrate that Ministries have documented and validated erasure procedures to ensure a thorough erasure of removable media commensurate with the sensitivity classification.
• Demonstrate all removable media marked for disposal is logged, tracked and kept secure (locked cabinet, safe room).
• Demonstrate that assets are removed from inventory at time of disposal and proper records are maintained.
• Demonstrate that employees are aware of secure media handling and disposal procedures.

1.3.3 Media being physically transported must be appropriately protected.
a) Media transport procedures

**Purpose:** To protect information from unauthorized disclosure or loss during physical transport of media.

1.3.3 a) Media transport procedures
The Office of the Government Chief Information Officer must document and implement security measures for the protection of media during transport that meet information classification and handling requirements. If information of various classifications is stored on media, the media must be protected according to the highest classification of the information stored.

Minimum media transport requirements are:
- Using couriers that are approved by government;
- Inspecting identification credentials of couriers upon pickup and delivery of packages;
- Obtain and retain receipts for media shipments;
- Using packaging that will protect the media from loss or damage; and,
- Packaging so that the classification of the media is not displayed.

Responsibility for specification of physical transport procedures are shared between Corporate Information and Records Management Office, the Risk Management Branch and Government Security Office.

**Guidelines:**
Where supported by a Security Threat and Risk Assessment, additional controls to protect media during transport include:
- Using notifications of transport activities, such as:
  - sender informing receiver of the impending shipment, and,
  - receiver confirming receipt of the shipment;
- Using two layers of packaging where the inner layer indicates the classification and handling requirements; and,
- Using a locked container.

**Recommended Tests:**
*Note: 1.3.3 is reported on as part of the annual information security review.*
- Demonstrate shipment logs are maintained and tracked to ensure delivery.
- Demonstrate that physical transport requirements are followed to prevent unauthorized disclosure or loss of media.