BRITISH COLUMBIA | Ministry of Citizens' Services

# PHYSICAL AND ENVIRONMENTAL 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 PHYSICAL AND ENVIRONMENTAL SECURITY** ....................................................................4

**1.1 SECURE AREAS** .....................................................................................................4

**1.2 EQUIPMENT SECURITY** ..........................................................................................10

## 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 Physical and Environmental Security

This chapter identifies requirements for protection from environmental and man-made threats to employees and property. One of the principles used for protection is the use of a layered defence, with perimeters and security zones that place computers, people and information in secure areas.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the security of government information and information systems.

## 1.1 Secure areas

| | |
|---|---|
| **1.1.1** | **Government information processing facilities must be protected by a physical security perimeter.**<br>**a) Security perimeter**<br>**b) Maintenance** |

***Purpose:*** ***To prevent unauthorized physical access to government information processing facilities.***

### 1.1.1 a) Security perimeter

Information Owners must ensure that the perimeters of an information processing facility are physically sound in design and consider landscaping, lighting, fencing, and closed-circuit television on the access routes to the building; that the roof, walls and flooring are of solid construction; and that exterior access points, windows, and doors are equipped with appropriate security controls (e.g., locks, alarms, bars).

All information processing facilities are a Restricted Access Security Zone.

Appropriate security controls must be applied to reduce the level of identified risks and include:

- A structure that prevents external visual and audio observations and complies with all applicable building codes for structural stability (external walls, internal walls, ceilings and doors). Walls surrounding the facility must be extended from true floor to true ceiling (slab to slab), to prevent unauthorized entry and minimize environmental contaminations such as that caused by fires and floods. Appropriate control mechanisms (e.g., locks, alarms and bars on windows and doors) must be applied to prevent unauthorized access;
- All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring employees to take immediate action;
- Information processing facilities must be equipped with doors that close automatically. These doors must set off an audible alarm when kept open beyond a certain period of time;
- All fire doors must be equipped with crash bars to allow a quick exit in the event of an emergency. When the doors are opened, an audible alarm may also be set off;
- Alarm systems must be continuously monitored (i.e., 24 hours a day, 7 days a week); and,
- Government information processing facilities must be physically separated from those managed by third parties.

### 1.1.1 b) Maintenance

Information Custodians must review, and where appropriate test, physical security and environmental control requirements at least annually.  Security requirements for facilities must be evaluated prior to significant:

- Alteration to exterior building layouts;
- Changes to perimeter security controls;
- Change in operations; and,
- As part of any related security incident investigation.

**Guidelines:**
The following guidelines support physical and environmental security by establishing perimeter security for information processing facilities:

- Information processing facilities should have a manned reception area to control access to the facility where feasible;
- Common service spaces such as eating areas, washrooms, cloakrooms, boardrooms and storage areas should be located so that they cannot be used to circumvent physical security;
- Visitor reception should be separate from entrance areas but provide an unobstructed view of the entrance; and,
- When physical security is outsourced, the contract must require that contracted employees are security screened and bonded.

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

- Demonstrate the perimeters of processing facilities are protected by intrusion devices.
- Demonstrate access to facilities is minimized and monitored (e.g., fire doors are alarmed).
- Demonstrate access to restricted zones is controlled (e.g., manned reception area, key-card access).
- Demonstrate regular review of information processing facility and records management storage rooms (e.g., computer data center or telecommunications equipment room or records management office).
- Provide the annual security /environmental control review and inspect to ensure they have fulfilled this requirement.

| | |
|---|---|
| **1.1.2** | **Secure areas must be protected by appropriate entry controls to ensure that only authorized employees are allowed access.**<br>**a) Entry controls**<br>**b) Maintenance** |

***Purpose:*** ***To prevent unauthorized physical access to government information.***

**1.1.2 a) Entry controls**
Information Owners and Information Custodians must establish the appropriate type and number of restricted zones to achieve the necessary conditions for employee safety and for the protection of sensitive or valuable information and assets.  Establishment of restricted zones must be supported by a Security Threat and Risk Assessment.

Access to any government information processing facility or areas where sensitive information is kept must be restricted.  Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone. Entry controls must identify, authenticate and log all access attempts to a Restricted Access Operations Zone or a Restricted Access Security Zone as follows:

- Restricted Access Operation Zone access is limited to ministry employees and their escorted visitors (i.e., standard working areas, conference rooms, offices); and,
- Restricted Access Security Zone access is limited to authorized employees and their escorted visitors (i.e., communication closets, server rooms).

Every person authorized to enter a facility, including visitors, must be issued an identification badge that contains identifying information (such as name and photograph) and their level of building access. Badge colour or some other bold identifier may be used to represent the level of access.

- All badges must be checked prior to entry. A receptionist, security guard or electronic reader that logs the identity, time, date, and access privileges of each entry attempt must do such checking. Entry control may be achieved using keys, proximity card readers or other technologies;
- Employees must challenge anyone in a secure area who is not displaying an identification badge;
- Visitor or temporary access badges must be returned and accounted for at the end of each day;
- Entry logs must be reviewed on a quarterly basis;
- All entry logs must be secured and maintained according to the approved records retention schedule for the system or information asset; and,
- Access rights to secure areas must be reviewed and updated regularly.

When physical security is outsourced (i.e., the use of security guards) the contract must require that contracted employees are security screened and bonded.

**1.1.2 b) Maintenance**

Information Custodians are responsible for reviewing physical entry control requirements annually. All entry controls in place must be tested annually. Security requirements for facilities must be evaluated and a Security Threat and Risk Assessment completed prior to:

- Alteration to interior building layouts;
- Change to equipment/systems located in the facility;
- Change in operations; and,
- As part of any related security incident investigation.

**Guidelines:**

The following guidelines support physical and environmental security by establishing security within information processing facilities:

- Common service spaces such as eating areas, washrooms, cloakrooms, boardrooms and storage areas should be located so that they cannot be used to circumvent physical security;
- Visitor reception should be separate from entrance areas but provide an unobstructed view of the entrance; and,
- When physical security is outsourced, the contract must require that contracted employees are security screened and bonded.

The effective use of restricted access zones in an open office environment depends on the implementation of appropriate security procedures, which may include:

- Respecting the need-to-access principle and zone perimeters;
- Escorting visitors;

- Securing sensitive or valuable information and assets when leaving the work areas; and,
- Taking precautions when discussing sensitive information.

**Recommended Tests:**
*Note: 1.1.2 is reported on as part of the annual information security review.*

- Demonstrate that layered zones are employed to protect information and information processing facilities (e.g., reception zone, operation zone and security zone).
- Demonstrate that access to restricted operational and security zones employs controls that identify, authenticate and monitor all access attempts.
- Demonstrate that access controls and alarm systems have been implemented, and active monitoring is performed with log records retained.
- Demonstrate regular entry controls testing to determine if they meet the requirements.

| | |
|---|---|
| **1.1.3** | **Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility.**<br>**a) Physical security requirements** |

***Purpose:*** ***To enhance physical and environmental security of information processing facilities by considering all security requirements during the design of the facility.***

**1.1.3 a) Physical security requirements**
Information Owners must design, document and approve security controls for information processing facilities based on a Security Threat and Risk Assessment. Considerations must include:

- Determining security perimeter and maintenance factors;
- Considering the operational use and information processing requirements of the facility;
- Establishing appropriate security zones;
- Design and construction complying with health and safety regulations and standards;
- Designed with environmental controls for the protection of information assets (e.g., fire suppression, HVAC, generators, alarms);
- Selecting unobtrusive sites and keeping signage to the minimum required for meeting fire and other safety requirements;
- Limiting the identification of critical information processing facility locations, in publicly and internally available directories, to the minimum required; and,
- Selecting sites so that public access to highly sensitive or critical locations can be strictly controlled or avoided.

**Recommended Tests:**
*Note: 1.1.3 is reported on as part of the annual information security review.*

- Demonstrate layered physical security measures.
- Demonstrate Security Threat and Risk Assessment(s) completed to ensure the room(s) conforms to the Physical Security Technical Standards for Secure Zones.
- Demonstrate security controls methodology and documentation.
- Demonstrate public access to sensitive security zones is restricted.

**1.1.4 Physical protection against natural disasters, malicious attacks or accidents must be designed and applied.**
**a) Design and site selection**

***Purpose:*** ***To enhance physical and environmental security by designing and applying physical security controls to mitigate damage from natural or man-made disaster.***

**1.1.4 a) Design and site selection**

Information Owners and Information Custodians, site planners and architects must incorporate physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural disasters, malicious attacks and accidents. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to meeting building code specifications and fire regulations, the following must be considered:

- Combustible or hazardous materials must be stored in purposely designed rooms and in appropriate containers;
- Installing intrusion detection and environmental alarm systems, fire suppression and firefighting systems must be included in the design phase; and,
- Fallback equipment (e.g., for Disaster Recovery Plan) and backup media must be sited at a safe distance to avoid damage from a disaster affecting the main site.

**Recommended Tests:**

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

- Demonstrate regular inspections of the information processing facility by managers, fire and safety experts are performed to ensure the facility work areas and public areas are safe for occupants and equipment (e.g., intrusion and environmental alarm systems, fire suppression and firefighting systems are installed and functional).
- Demonstrate combustibles or hazardous materials are stored in approved containers separate from secure areas.
- Demonstrate appropriate alarms are situated for noxious gases, fire and flood and are monitored 24/7.
- Demonstrate system redundancy is sited at a safe distance in order to avoid damage affecting primary site.

**1.1.5 Security controls and procedures must be used by employees working in secure areas.**
**a) Secure area requirements for employees**
**b) Other secure area requirements**

***Purpose:*** ***To prevent unauthorized physical access to government information by designing and applying additional security controls and procedures for employees working in secure areas.***

**1.1.5 a) Secure area requirements for employees**

Information Owners and Information Custodians must identify and document requirements that apply to employees authorized to work in secure areas. Information Owners must ensure that background checks including criminal records reviews are conducted for employees working in secure areas.

Information Owners and Information Custodians are responsible for informing employees working within a secure area that:

- Activities within a secure area are confidential and must not be discussed in a non-secure area - sensitive information must not be discussed with persons without a need-to-know;
- No type of photographic (including cameras in mobile devices), video, audio or other recording equipment is to be operated in a Restricted Access Security Zone unless authorized; and,
- Information security incidents must be reported immediately.

**1.1.5 b) Other secure area requirements**
Information Owners and Information Custodians must identify and document requirements for other individuals who may need access to a secure area. Information Owners and Information Custodians are responsible for ensuring that:

- Maintenance employees, cleaners and others who may require access on an ongoing basis to the secure area must be screened and their names placed on access lists;
- Visitors must obtain approval for visits, be screened, and their entry and departure times logged;
- Employees must escort visitors when they are within secure areas;
- Unoccupied secure areas must be physically locked and periodically checked; and,
- Physical intrusion alarms and detection devices must be installed to automatically alert monitoring employees of a breach.

**Recommended Tests:**
*Note: 1.1.5 is reported on as part of the annual information security review.*

- Demonstrate all employees who require access on an ongoing basis to secure areas are screened and their names placed on access lists; visitors obtain approval for visits, are screened, and their entry and departure times are logged.
- Demonstrate an escalation process to investigate any violation of policies or standards reported by the monitoring employees.
- Demonstrate controls for employees working within a secure area that include employees escort visitors when they are within the secure area; unoccupied secure areas are physically locked and periodically checked; physical intrusion alarms are installed to automatically alert monitoring employees of a breach.

**1.1.6 Access to delivery and loading areas must be controlled, and where possible, separated from information processing facilities.**
**a) Controlling access to delivery and loading areas**

***Purpose:*** ***To prevent unauthorized physical access to government information by controlling access to delivery and loading areas and separating them from information processing facilities whenever possible.***

**1.1.6 a) Controlling access to delivery and loading areas**
Information Owners and Information Custodians, planners and architects must ensure that access to delivery and loading areas or access from Reception Zones is controlled when considering building design and specifications. The following factors must be considered:

- Delivery and loading areas must be designed so that supplies can be unloaded without delivery employees gaining access to restricted access zones;
- Protection of the delivery and loading areas must begin at the perimeter with continuous monitoring in place (e.g., gated fence, CCTV, separation from public access);

- Access to delivery and shipping areas must be restricted to authorized employees only;
- Setting and maintaining hours of operation for delivery and pick-up;
- A combination of internal and external locking doors or gates must be used to provide security;
- Incoming and outgoing shipments should be segregated when possible;
- Incoming material must be inspected for potential threats before being moved to or from the delivery and loading area. Inspections can be undertaken randomly if resources are not available to inspect every package;
- Hazardous materials must be appropriately packaged and identified as to safety precautions;
- Bills of lading must be compared to goods delivered;
- Loading docks and delivery areas must be regularly inspected and actively monitored;
- Records must be kept for internal and external deliveries and shipments;
- Reception areas must confirm the identification of all visitors for restricted zone access; and,
- All visitors must be accompanied while in restricted operational and security zones.

For facilities that include delivery and loading areas, and/or reception zones, a Security Threat and Risk Assessment and inspection must be conducted to determine that access can be adequately controlled.

**Recommended Tests:**
*Note: 1.1.6 is reported on as part of the annual information security review.*

- Demonstrate logs are maintained for all deliveries and shipments.
- Demonstrate reception areas, receiving and shipping areas are monitored for unauthorized access.

## 1.2 Equipment Security

**1.2.1 Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards.**
**a) Equipment siting**
**b) Equipment protection**

***Purpose:*** ***To reduce risks to equipment from unauthorized access, environmental threats and hazards.***

**1.2.1 a) Equipment siting**
Information Owners, Information Custodians, planners, and architects must collaborate to ensure that the design and layout of information processing facilities provides protection for equipment from security threats as supported by a Security Threat and Risk Assessment. Safeguards must include:

- Locating servers and other centralized computing equipment within a Restricted Access Security Zone;
- Locating workstations, laptops and printers in a Restricted Access Operations Zone;
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas; and,
- Locating shared printers, scanners, copiers, and facsimile machines away from public or reception areas, or in passageways or other areas where employees who do not have a need-to-know can access printed material.

Information Owners and Information Custodians are responsible for ensuring that kiosks and public terminal safeguards are based on a Security Threat and Risk Assessment.

**1.2.1 b) Equipment protection**
Information Owners, Information Custodians, planners, and architects must collaborate to ensure that the design and layout of information processing facilities provides protection from physical and environmental hazards. Safeguards must include:

- Using equipment designed for suppression of electromagnetic emanations that may be used to capture information, when the need is supported by a Security Threat and Risk Assessment;
- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Providing lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Providing employees with approved eating and drinking areas separate from work areas containing equipment;
- Briefing employees who work with equipment about safety practices in the workplace and emergency equipment procedures to prevent an escalation in equipment damage;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems; and,
- Regularly inspecting the information processing facility(s) for integrity of ceilings, walls, windows, and other infrastructure for damage from water and other environmental factors that may pose a threat to safe equipment operation.

**Recommended Tests:**
*Note: 1.2.1 is reported on as part of the annual information security review.*

- Demonstrate the application of security zones.
- Demonstrate that equipment is properly sited and protected.
- Demonstrate temperature and heating are monitored to protect against adverse effects on equipment.
- Demonstrate that kiosk and public terminal safeguards are reviewed.
- Demonstrate that periodic inspections are conducted.

| | |
|---|---|
| **1.2.2** | **Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.**<br>**a) Planning and design**<br>**b) Maintenance** |

***Purpose:*** ***To ensure continued availability by protecting equipment from disruptions caused by failures in supporting utilities.***

**1.2.2 a) Planning and design**
Information Owners and Information Custodians, planners, architects and engineers must collaborate in the planning and design of an information processing facility to ensure that supporting utilities (e.g.,

water, power, sewage, heating, ventilation) are adequate to support employees and systems that will be located in the facility. This includes estimating current and future utility capacity requirements for the facility. In addition to meeting the building code and other regulations, the following must be included in facility planning and specifications:

- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements;
- Emergency power off switches located near emergency exits in equipment rooms;
- Emergency lighting;
- Alarms to indicate inadequate water pressure for fire suppression;
- Alarms to indicate malfunctions in heating, ventilation, air conditioning, humidity control and sewage systems;
- Multiple connections to the power utility for critical systems and equipment;
- Multiple telecommunications connections to prevent loss of voice services; and,
- Adequate voice communications to meet regulatory requirements for emergencies.

**1.2.2 b) Maintenance**

Information Custodians must ensure that facilities are inspected regularly in accordance with building codes and other regulations. Evacuation and other emergency drills must be practiced regularly in collaboration with fire and emergency services. The facility requirements for utilities shall be re-evaluated:

- During the planning phase for replacing or changing existing technology hardware;
- When moving significant numbers of new employees into facilities;
- During the planning of renovations or major changes to an existing facility;
- Prior to leasing a facility; and,
- When there are major changes to the surrounding area that may affect utilities, evacuation routes or other safety aspects.

**Recommended Tests:**

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

- Demonstrate redundancy in design for electric power, HVAC, water and communications.
- Demonstrate that Uninterrupted Power Supply (UPS) systems are tested regularly (e.g., monthly or quarterly), backup generators are tested regularly, and fuel supplies are maintained and replenished.
- Demonstrate facilities are inspected regularly in accordance with building codes and other regulations.
- Demonstrate evacuation and other emergency drills are practiced regularly in collaboration with fire and emergency services.

**1.2.3 Power and telecommunications cabling must be protected from interception and damage.**
**a) Protection**
**b) Inspection and monitoring**

***Purpose:*** ***To ensure continued availability and integrity of information systems and information processing facilities by protecting power and telecommunications cabling from interception and damage.***

**1.2.3 a) Protection**

Information Owners and Information Custodians, planners and architects must include the protection of power and telecommunications cabling from interception and damage when designing or leasing facilities. The following methods to increase protection must be considered:

- Access to communication closets and server rooms must be highly restricted;
- Power and telecommunications cabling must be underground and/or in a secure conduit;
- Information cabling other than fibre optic must be protected with electromagnetic shielding when required;
- When supported by a Security Threat and Risk Assessment, consideration must be given to the use of fibre optics for telecommunications cabling;
- Cables must not be accessible in public areas;
- Power and telecommunications cabling must be segregated in accordance with building codes and other regulations; and,
- Inspection boxes, termination points, patch panels, control rooms and other facilities must be secured and located inside a Restricted Access Security Zone.

**1.2.3 b) Inspection and monitoring**

Information Custodians must ensure that:

- The integrity of power and telecommunications cables are monitored through regular inspections and reports;
- Power cabling and telecommunication schematics and documentation must be maintained in order to support inspections;
- Records of patches and other changes are maintained and inspected; and,
- Power and telecommunications cabling and wiring closets are inspected regularly and monitored for unauthorized access or inappropriate activity. The frequency of monitoring activities must be supported by a Security Threat and Risk Assessment.

**Recommended Tests:**

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

- Demonstrate that the inspection of power and telecommunications cabling is performed annually.

**1.2.4 Equipment must be correctly maintained to enable continued availability and integrity.**
**a) Routine maintenance**
**b) Maintenance of systems, hardware or media containing government information**

***Purpose:*** ***To ensure the continued confidentiality, integrity and availability of equipment through correct maintenance.***

**1.2.4 a) Routine equipment maintenance**

Equipment being repaired or maintained must be protected commensurate with the sensitivity of the information it contains and the value of the equipment. Information Owners and Information Custodians must determine if repair or maintenance can be conducted off-site. The need to protect sensitive information may justify equipment destruction and replacement rather than repair or maintenance. Information Custodians are responsible for:

- Ensuring the scheduling of routine, preventive maintenance of equipment by qualified, authorized employees;

- Ensuring that maintenance is performed in accordance with the manufacturer's specifications, in compliance with warranty requirements, and using safe practices as specified in building codes, other regulations and insurance policies;
- Ensuring that, where possible, maintenance is scheduled to avoid interference with services or operations;
- Notifying affected employees prior to taking equipment off-line for scheduled maintenance;
- Ensuring that the value and sensitivity of the information contained on the device is considered prior to approval of off-site maintenance;
- Equipment sent for off-site maintenance must be inspected and logged out;
- Ensuring equipment returning from off-site repair or maintenance is inspected and logged in;
- Maintaining detailed records to identify trends, weaknesses and additional maintenance requirements which must include:
  - Place, date, time, type of scheduled maintenance and technical employees,
  - Suspected and actual faults identified,
  - Diagnostics performed, and corrective action taken,
  - Unusual or unexpected events, such as early failures or breakdowns, and,
  - Any other event that requires maintenance.
- Ensuring maintenance on critical equipment is undertaken in such a manner that the system is not off-line due to scheduled maintenance; and,
- Ensuring that when equipment is brought back on-line after scheduled maintenance that all operational specifications are satisfactory.

**1.2.4 b) Maintenance of systems, hardware or media containing government information**
Information Custodians must consult with Information Owners regarding the value and sensitivity of the information stored on hardware or media when determining whether repairs will be conducted. Information Custodians must ensure that information is safeguarded:

- Maintenance on critical systems must be undertaken in such a manner that the system is not off-line due to scheduled maintenance;
- Hardware or media sent for repairs or maintenance outside of the information processing facility must do so through pre-approved and screened bonded couriers;
- Hardware or media containing confidential or personal information must not have maintenance or repairs conducted off-site;
- Hardware or media containing confidential or personal information that cannot be repaired on-site must be destroyed in accordance with approved disposal standards commensurate with the sensitivity of the information held;
- Maintenance must be factored into system availability requirements; and,
- Repair or maintenance must be conducted within Canada.

**Recommended Tests:**
*Note: 1.2.4 is reported on as part of the annual information security review.*

- Demonstrate that Ministry-specific equipment maintenance logs are up-to-date (e.g., MFD service logs) and/or there is a maintenance schedule maintained, or contracts include scheduled maintenance, and that the maintenance has been conducted.
- Demonstrate that only qualified authorized employees carry out maintenance and repairs in accordance with supplier recommended service intervals and specifications.
- Demonstrate any equipment taken off-site is in a secure state and that no information is vulnerable to loss or unauthorized access.

- Demonstrate service contracts include schedules of regular maintenance activities.
- Demonstrate there a process to ensure the maintenance activities are completed.

| | |
|---|---|
| **1.2.5** | **Equipment, information or software belonging to the Province must not be removed from government premises without prior authorization.**<br>**a) Authorized removal of assets** |

***Purpose:*** ***To protect assets belonging to the Province from unauthorized removal.***

**1.2.5 a) Authorized removal of assets**

Information Owners and Information Custodians must establish a formal authorization process for the removal of assets for re-location, loan, maintenance, disposal or any other purpose. Authorization forms for asset removal must include:

- Description and serial numbers;
- Information about where the asset will be located;
- The removal date and return date;
- The identity of the individual responsible for the asset; and,
- Reason for removal of the asset.

The description and serial numbers must be verified when the asset is returned.

Employees must be informed of, and accept responsibility for, protection of the asset (e.g., Terms and Conditions of Use).

**Recommended Tests:**

*Note: 1.2.5 is reported on as part of the annual information security review.*

- Demonstrate the use of authorization forms for asset removal.
- Demonstrate a regular review of equipment inventory check-out and check-in lists matching requests and authorization, purpose (e.g., loan, maintenance), asset information (e.g., serial numbers), current location and custodian contact information.
- Demonstrate employee awareness of controls for removing information assets and acceptance of responsibility.

| | |
|---|---|
| **1.2.6** | **Equipment must be protected using documented security controls when off-site from government premises.**<br>**a) Security controls** |

***Purpose:*** ***To protect equipment in the custody of employees from loss or unauthorized access.***

**1.2.6 a) Security controls**

Information Owners and Information Custodians must ensure that equipment being used off-site to access government information is protected commensurate with the sensitivity and the value of the information it contains. Information Custodians must ensure that:

- Sensitive data is encrypted;
- Equipment is protected from unauthorized access by the use of a logical or physical access control mechanism (e.g., password, USB key or smart card);
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and,
- Employees are familiar with operation of the protection technologies in use.

To provide further protection employees must:

- Not leave equipment unattended in a public place;
- Ensure that equipment is under their direct control at all times when travelling;
- Use the physical locking, restraint or security mechanisms provided by the Information Custodian whenever possible;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and,
- Report loss of equipment immediately using the Information Incident Management Process and General Incident or Loss Report (GILR).

**Recommended Tests:**
*Note: 1.2.6 is reported on as part of the annual information security review.*

- Demonstrate in cases of sensitive information that encryption is in place and the device is protected by password or other authentication.
- Demonstrate that employees are made aware of their responsibilities for securing off-site equipment.
- Demonstrate area specific threats are considered prior to authorization for travel outside of Canada.

**1.2.7 Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed.**
**a) Reassignment of hardware and media**
**b) Destruction of hardware**

***Purpose: To protect information from unauthorized disclosure.***

**1.2.7 a) Reassignment of hardware and media**

Information Owners must consider the value and sensitivity of the information stored on hardware or media when determining whether it will be reassigned within government or destroyed. Reassignment must only occur within or between government ministries. Prior to reassignment of hardware or media, Information Owners and Information Custodians must ensure:

- The integrity of government records is maintained by adhering to Records Management policies;
- Information and software are erased using methods and standards approved by the Office of the Government Chief Information Officer;
- Roles and responsibilities are documented; and,
- Asset inventories are updated to record details of the erasure and reassignment including:
  - Asset identifier,
  - Date of erasure,
  - Names of employees conducting the erasure,
  - Date of transfer, and,
  - Name of new asset custodian.

Where information is erased by third parties there must be contractual and audit procedures to ensure complete destruction of the media. Third parties must certify that destruction has occurred.

**1.2.7 b) Destruction of hardware**

Information Owners and Information Custodians are responsible for ensuring hardware media used to store information or software is destroyed in a secure manner. Corporate Information and Records Management Office is responsible for ensuring secure disposal or destruction services are available to Information Owners and Information Custodians.

**Guidelines:**
A Corporate Supply Arrangement exists for provision of secure media destruction services. Secure destruction service companies must be used to perform media disposal. Contact the Ministry Records Officer for further details.

**Recommended Tests:**
*Note: 1.2.7 is reported on as part of the annual information security review.*

- Demonstrate the ministry, division, or branch maintain records of IT assets sent for disposal.
- Demonstrate that the information classification of assets being disposed is either the highest sensitivity of the information contained within or capable of being processed by the asset.
- Demonstrate that when information is erased by third parties there are contractual and audit procedures to ensure complete destruction of the information.

**1.2.8 Employees must ensure unattended equipment has appropriate protection.**
**a) Protection of unattended equipment**

***Purpose:*** ***To reduce risk of unauthorized access, loss or damage to information and information systems.***

**1.2.8 a) Protection of unattended equipment**
Information Owners must ensure that employees are aware of their responsibilities to secure unattended equipment to prevent unauthorized access to information systems by:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling password protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password protection on mobile devices including portable storage devices; and,
- Being aware of their responsibility to report security weaknesses where the above controls have not been applied.

B.C. Government workstations and other devices used for information system access must automatically activate screen savers or equivalent locking systems after 15 or less minutes of inactivity.

**Recommended Tests:**
*Note: 1.2.8 is reported on as part of the annual information security review.*

- Demonstrate that information systems have a default timeout and are password protected.
- Demonstrate that the requirements to secure unattended equipment are communicated to employees.
- Demonstrate that mobile devices can be wiped remotely.

**1.2.9 Employees must ensure the safety of sensitive information from unauthorized access, loss or damage.**
**a) Securing the work space**
**b) Secure work habits**

***Purpose:*** ***To reduce risk of unauthorized access, loss or damage to information by ensuring employees take reasonable security precautions.***

### 1.2.9 a) Securing the work space

Employees must secure their work space whenever it is not supervised by an authorized person, including during short breaks, attendance at meetings, and at the end of the work day.
Securing the work space includes:

- Clearing desk tops and work areas;
- Securing documents and mobile or portable storage devices in a locked desk or file cabinet;
- Ensuring outgoing and incoming mail is appropriately secured;
- Enabling a password protected screen saver;
- Shutting down and restarting workstations at the end of each work day;
- Locking doors and windows; and,
- Checking fax machines and printers to ensure that no sensitive information is waiting to be picked up.

### 1.2.9 b) Secure work habits

Employees must develop and implement security conscious work habits to reduce the likelihood of unauthorized viewing, access or disclosure of sensitive information.
Security conscious work habits include:

- Ensuring sensitive information is protected from accidental viewing by persons passing through the work space;
- Ensuring that only the documents required for current work are out of their normal file cabinet;
- Ensuring white boards, bulletin boards, flip charts do not contain sensitive information when the viewing audience cannot be defined;
- Covering up, filing or storing paper documents when visitors are present in the work area;
- Clearing, changing or turning off the computer screen (e.g., minimize open Windows) so that sensitive information is not displayed when visitors are present in the work area; and,
- Not discussing sensitive information in open work spaces or public areas.

**Guidelines:**

Ensure that offices can be locked and that storage with locks is available.

**Recommended Tests:**

*Note: 1.2.9 is reported on as part of the annual information security review.*

- Determine if information systems have a default timeout and are password protected.
- Determine information systems are sited in a secure zone that limits access to authorized users.
- Demonstrate employee awareness of responsibilities and requirements to report security weaknesses.