Physical and Environmental Security Standard

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan Physical and Environmental security standards.

Table of Contents

Reference Documents

The following documents are available on the IT Security Services Taskroom:

- *Physical and Environmental Security Policy*

1. Secure Areas

1.1. Physical Security Perimeter

A secure area may be a lockable office, or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.

Controls that must be applied are:

- security perimeters must be clearly defined, and the siting and strength of each of the perimeters must depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
- perimeters of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site must be of solid construction and all external doors must be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks, etc.; doors and windows must be locked when unattended and external protection must be considered for windows, particularly at ground level;
- a manned reception area or other means to control physical access to the site or building must be in place; access to sites and buildings must be restricted to authorized personnel only;
- physical barriers must, where applicable, be built to prevent unauthorized physical access and environmental contamination;
- all fire doors on a security perimeter must be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they must operate in accordance with local fire code in a failsafe manner;
- suitable intruder detection systems must be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas must be alarmed at all times; cover must also be provided for other areas, e.g. computer room or communications rooms;
- information processing facilities managed by the organization must be physically separated from those managed by external parties.

Special consideration must be given towards physical access security when the facility houses multiple organizations.

1.2. Physical Entry Controls

The following controls must be implemented:

- access to areas where sensitive information is processed or stored must be restricted to authorized personnel only;
- authentication controls, e.g. access control card system, must be used to authorize and validate all access;
- an audit trail of all access must be maintained;
- visitors must be escorted by authorized personnel;
- visitors must only be allowed access for specific and authorized purposes;
- the date and time of entry and departure of visitors must be recorded;
- all employees and other authorized personnel must wear visible identification;
- visitors must be issued badges or tags of a different colour than employees;
- employees must notify security personnel when they encounter unescorted visitors or anyone not wearing visible identification;
- external party support personnel may be granted restricted access only when required; their access must be authorized and monitored; and
- access rights must be regularly reviewed, updated, and revoked when necessary.

1.3. Securing Offices, Rooms and Facilities

Controls that may be implemented to reduce associated risks are:

- physical entry controls;
- ensuring sensitive information is stored properly when not in use; and
- ensuring that directories that identify the locations of data centres and other areas where sensitive information is stored are not be made public.

1.4. Protecting Against External and Environmental Threats

Designs must incorporate – to the extent possible – physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural and man-made disaster. Consideration must also be given to any security threats presented by neighbouring premises or streets. In addition to building code and fire regulations:

- combustible or hazardous materials must be stored at a safe distance from the secure area;
- bulk supplies, e.g. stationary, must not be stored in a secure area;
- fallback equipment and backup media must be located off-site at a safe distance to avoid damage from a disaster affecting the main site; and
- environmental alarm systems, fire suppression and firefighting systems must be installed.

1.5. Working in Secure Areas

Authorized personnel working a secure area must be informed that:

- sensitive information cannot be discussed in a non-secure area;
- sensitive information cannot be disclosed to personnel who do not have a need-to-know;

- no type of photographic, smartphone, video, audio or other recording equipment can be brought into a secure area unless specifically authorized;
- maintenance staff, cleaners and others who require periodic access to the secure area must be screened and their names added to an access list; and
- visitors must be authorized, logged and escorted.

1.6. Delivery and Loading Areas

Physical security controls for delivery and loading areas must ensure that:

- access to a delivery and loading area from outside of the building must be restricted to identified and authorized personnel;
- the delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
- the external doors of a delivery and loading area must be secured when the internal doors are opened;
- loading docks and delivery areas must be regularly inspected and actively monitored;
- incoming material must be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
- incoming material must be registered in accordance with asset management procedures on entry to the site; and
- incoming and outgoing shipments must be physically segregated where possible.

2. Equipment

2.1. Equipment Siting and Protection

Physical siting controls must ensure that:

- servers, routers, switches and other centralized computing equipment must be located in a room with access restricted to only those personnel who require it;
- workstations, laptops, digital media and storage devices must be located and used in an area that is not accessible to the public;
- equipment must be located, and monitors angled, in such a way that unauthorized persons cannot observe the display;
- shared printers, scanners, copiers and fax machines cannot be located in an area that is accessible to the public; and
- kiosks and other devices that are intended for public use must be clearly labelled and placed in a publicly accessible area.

2.2. Supporting Utilities

The following controls must be implemented to help ensure availability of critical services:

- All supporting utilities such as electricity, water supply, sewage, heating/ventilation and air conditioning must be adequate for the systems they are supporting. Support utilities must be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply must be provided that conforms to the equipment manufacturer's specifications.

- An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans must cover the action to be taken on failure of the UPS. A back-up generator must be considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel must be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators must be regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer's recommendations. In addition, consideration could be given to using multiple power sources or, if the site is large, a separate power substation.
- Emergency power off switches must be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting must be provided in case of main power failure.
- The water supply must be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used). Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively. An alarm system to detect malfunctions in the supporting utilities must be evaluated and installed if required.
- Telecommunications equipment must be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services must be adequate to meet local legal requirements for emergency communications.

2.3. Cabling Security

The following controls must be implemented to help ensure security of critical cabling:

- Power and telecommunications lines into information processing facilities must be underground, where possible, or subject to adequate alternative protection.
- When identified in a Threat and Risk Assessment, network cabling must be protected from unauthorized interception or damage by using a conduit and by avoiding routes through public areas.
- Power cables must be segregated from communications cables to prevent interference.
- Cables and equipment must be clearly marked to minimize handling errors such as accidental patching of wrong network cables. A documented patch list must be used to reduce the possibility of errors.
- When a Threat and Risk Assessment finds a need for more safeguards, consider:
    - installation of rigid conduit and locked rooms or boxes at inspection and termination points;
    - use of alternative routings and/or transmission media providing appropriate security;
    - use of fibre optic cabling;
    - use of electromagnetic shielding to protect the cables;
    - initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables; and
    - controlled access to patch panels and cable rooms.

2.4. Equipment Maintenance

When equipment is serviced, Information Owners must consider the sensitivity of the information it holds and the value of the assets. The following controls must be applied:

- equipment must be maintained in accordance with the supplier's recommended schedule and specifications;
- only authorized maintenance personnel may carry out repairs and service equipment;
- records must be kept of all suspected faults and all preventive and corrective maintenance;
- maintenance must be scheduled at a time of day that limits interference with services or operations;
- users must be notified before equipment is taken off-line for maintenance;

If off-site maintenance is required, then the asset must be cleared of all sensitive information. If it's not possible to de-sensitize assets before sending for maintenance, then the Ministry Security Officer and Information Owner must consider destruction of the asset.

2.5. Removal of Assets

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

- item description and serial number(s);
- information indicating where the asset will be located;
- the removal date and return date;
- the name of the individual responsible for the asset; and
- the reason for removal.

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

2.6. Security of Equipment and Assets Off-Premises

Information Owners must ensure that equipment used or stored off-site is safeguarded in accordance with the sensitivity of the information and the value of the assets. Controls to apply include:

- encrypt sensitive data when determined by a Threat and Risk Assessment;
- use a logical or physical access control mechanism (BIOS password, USB key, smart card) to protect against unauthorized access;
- use a physical locking or similar mechanism to restrain the equipment;
- ensure personnel are instructed on the proper use of the chosen controls.

Personnel in possession of government equipment:

- must not leave it unattended in a public place;
- must ensure the equipment is under his/her direct control at all times when traveling;
- must take measure to prevent viewing of sensitive information by unauthorized personnel;
- must not allow other persons to use the equipment;
- must report loss or stolen equipment immediately.

2.7. Secure Disposal or Re-Use of Equipment

Prior to re-use within government:

- the integrity of government records must be maintained by adhering to Records Management standards and policies;
- information and software must be backed up by the original Information Owner; and
- the storage media must be wiped in accordance with Asset Management Security Policy and Standards.

Storage media that will no longer be used in government must be wiped by a method approved by the Executive Director, Information Security Branch, in compliance with Asset Management Security Policy and Standards. Asset inventories must be updated to record details of the data wiping including:

- asset identifier;
- date of erasure;
- names of personnel conducting the erasure.

When a supplier conducts the data wiping there must be contractual and audit procedures to ensure complete destruction of the information. The government must receive certification that the destruction has occurred.

2.8. Unattended User Equipment

Users must safeguard unattended equipment by:

- terminating the active session when finished;
- locking the session with a password protected screen saver or other approved mechanism;
- logging off computers, servers, mainframes and other devices when the session is finished;
- enabling password protection on mobile devices and portable storage devices; and
- securing devices with a cable lock when enhanced physical security is justified.

2.9. Clear Desk and Clear Screen Standard

Users must secure their work spaces when it cannot be monitored by authorized personnel by:

- clearing desktops and work areas;
- locking hard copy sensitive information in an appropriate cabinet;
- locking portable storage devices with sensitive information in an appropriate cabinet;
- activating a password-protected screen saver;
- safeguarding incoming and outgoing mail;
- retrieving documents from printers and fax machines; and
- ensuring that sensitive hard copy documents no longer needed are placed in shredding bins, not recycle bins.

When visitors, cleaning staff or other personnel without a “need-to-know” are in the area, safeguard sensitive information by:

- covering up and maintaining control of hard copy files; and
- blanking computer screens or activating the password-protected screen saver.