REFERENCE GUIDE

Physical security measures for facilities

June 2019

Table of contents

Target audience

This document is intended for small- and medium-sized enterprises (SMEs) that want to implement physical security measures to protect their assets.

This is not an exhaustive list, rather a summary of the main points to consider and take into account when developing a physical security plan for an organization.

All physical security measures and procedures should comply with applicable laws and codes.

Physical security – Rationale, principles and objectives

Physical security includes all the safeguards used to ensure that assets (information, property and facilities) are protected from unauthorized access, disclosure, modification or destruction, in accordance with their level of sensitivity, criticality and value.

The value of an asset is the level of harm that would result if the asset's integrity, accessibility or availability were compromised.

Assets to be protected

Assets come in different forms:

- Tangible (e.g., high-value equipment)
- Intangible (e.g., intellectual property, confidential information)
- Mixed (e.g., employees)

Implementation

Organizations can use the following procedure to adapt the security measures to be implemented:

1. Identify the assets
2. Determine the value of the assets
3. Prioritize the assets based on value
4. Determine the threats and vulnerabilities of each asset
5. Determine the safeguards to implement for each asset

Crime prevention principles

Physical protection measures and systems should be implemented using crime prevention principles.

Principle	Objective
Deter	Create an environment that shows that the risk of an attack failing is greater than the success of the goal pursued by the attacker.
Detect	• Detect an attack in progress • Notify a response team
Delay	Slow down malicious actors in achieving their goal to allow for an appropriate response to the attack.
Prevent	Prevent malicious actors from achieving their goal through • Effective deterrent measures • Timely interventions based on the type of attack

Crime Prevention Through Environmental Design (CPTED)

CPTED proposes effectively using the environment to observe intruders so as to reduce opportunities for crime and protect legitimate users. CPTED is based on principles applicable to buildings and their external environment.

Principles:

Natural surveillance

Maximize visibility (seeing and being seen) from surrounding public spaces.

- Seeing inside the building from outside
- Seeing outside the building from inside
- The external environment surrounding the building

Natural access control

- Direct people and vehicles to specific entry points
- Deter or prevent access using physical or symbolic barriers (signage)

Territorial reinforcement and demarking boundaries

- Clearly distinguish private spaces from public spaces
- Create a sense of ownership for legitimate users and occupants
- Increase the vigilance of legitimate users to spot malicious actors
- Indicate to malicious actors that they are not welcome (deterrence)

Show that the space is being used

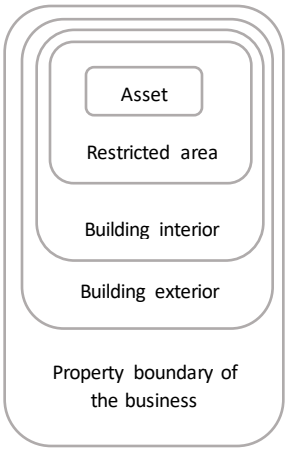
- Encourage legitimate activities on the premises
- Show that the space is being monitored
- Demonstrate a constant presence
- Ensure the premises are maintained

Security lighting (interior/exterior)

- Overlap lighting to reduce having unlit areas
- Standardize the lighting from one zone to another
- Limit glare effects

Defence-in-depth

- Create multiple layers of protection
- Protect critical assets behind multiple barriers
- Increase the time needed to commit an attack
- Establish a defense strategy based on several different complementary measures
- Give the time needed for a response



Building envelope – protecting openings

Most intrusions into buildings are done through doors and windows. If possible, openings should have an equivalent resistance to that of the walls.

Types of openings:

- Doors (hardware, door and frame materials, etc.)
- Windows (type of glass, anti-break film, bars, etc.)
- Other openings (ventilation louvers, hatches, etc.)

Access control

A technique that combines various methods of authorizing access to the entry points of an establishment or premises to protect people, information and property.

Access control can be applied:

- To staff, visitors and suppliers
- To some staff members for certain sensitive areas (offices, computer rooms)
- At all hours or at certain times of day or night
- To people, vehicles, goods

Access control principles

- Minimize the number of entry points to facilitate access control
- Clearly demarcate entry points with an easily identifiable perimeter such as a door or furniture arranged in a specific way
- Control access to all entry points to channel people and material entering

Access control methods

- Personal recognition (receptionist, security guard, colleague)
- Mechanical (combination lock or use of a controlled or uncontrolled key)
- Electronic (access card, keypad, biometrics)

Managing access rights

In order to ensure secure management of physical access, access to an area or an asset should only be granted if required by a person's duties, regardless of the person's status.

Managing access devices

An access device gives the holder the right to enter a controlled area (code, key, card, etc.)

- Keep the amount of access devices in circulation to a minimum
- Keep devices in a locked cabinet and limit access to those responsible for granting access devices
- In case of loss, theft or compromise, recode (reset) the locks and deactivate the card
- Maintain a log of access devices granted and in storage
- Do a periodic review of the access devices granted
- Review the access devices granted upon termination of employment, end of contract or change of duties

Managing visitors

Access control procedures should also be put in place for visitors. A visitor is a person who is not an employee of the organization and who needs to access an area reserved for employees. The goal is to prevent a visitor from accessing a restricted area without authorization.

- Establish a procedure for identifying and accompanying visitors
- Maintain a sign-in and sign-out log for visitors

Alarm system

An alarm system is a way to detect and communicate unusual activities in real time:

- Perimeter intrusion detection (door contacts, etc.)
- Volumetric intrusion detection (motion detectors, etc.)
- Fire and gas detection
- Personal assistance alert (medical emergency, duress, etc.)
- Monitoring of critical points (temperature, water level, etc.)

Best practices

- Establish alarm response procedures based on the type of alarm
- Have a backup system that provides protection for at least 24 hours in case of power failure
- Keep the number of users of the alarm system to a minimum

- Remove all users who are no longer needed upon termination of employment
- Assign authority levels according to the tasks to be performed
- Equip the alarm system with two modes of communication with the alarm control unit
- Periodically test the alarm system
- Install sirens inside

Video surveillance (CCTV)

CCTV can be a valuable part of an institution's security program. It is mainly used to:

- Detect activities that require a security response
- Collect images of an incident for later review and use as evidence if necessary
- Assist in the assessment of an incident

Ask the following questions to determine the functional requirements of a CCTV system:

- What is the goal of the system?
- What is each camera supposed to monitor?
- What are the requirements for real-time monitoring or image recording?
- What are the lighting constraints?

CCTV and privacy

Images and other information captured by a CCTV system is deemed to be personal information within the meaning of the law. Since video surveillance is a form of invasion of privacy, certain obligations must be met with respect to the collection and retention of personal information.

Buying tips

Here are some important points to keep in mind when requesting a quote from a security service provider.

- Ask for a detailed quote (parts, labour, travel, annual fees, etc.)
- Ask for plans indicating the location of the components
- Buy equipment that can be supported by different suppliers so you can switch suppliers without having to replace the equipment
- Ask about service delays in the event of malfunction

More information

More information can be found below:

- *Industrial Security Manual*, Government of Canada: https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-eng.html
- *Industrial Security Manual resources*, Government of Canada: https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/rssrcs-rsrcs-eng.html
- *G1-025 Protection, Detection and Response*, Royal Canadian Mounted Police: http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-025-eng.htm#7.1
- Asis: https://www.asisonline.org/