REFERENCE SHEET

PHYSICAL SECURITY MEASURES OF INSTALLATIONS

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, but 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 must comply with applicable laws and codes.

Physical security – Rationale, principles and objectives

Physical security includes all the safeguards used to protect assets (information, property and facilities) from unauthorized access, disclosure, modification, or destruction, based on their level of sensitivity, relevance, 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 can come in different forms:

- Tangible (e.g. very valuable equipment)
- Intangible (e.g. Intellectual property, confidential information)
- Mixed (e.g. employees)

Implementation

Each organization can apply the security measures to be implemented differently by following this procedure:

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 put in place for each asset

Crime prevention principles

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

Principle	Objective
Deter	Create an environment that demonstrates that the risk of an attack failing outweighs the probability of the attacker succeeding.
Detect	• Detect an attack in progress • Notify a response team
Delay	Slow down malicious parties in achieving their goal to allow for an appropriate response to the attack.
Prevent	Prevent malicious parties from achieving their goal through: • Effective deterrent measures • Timely interventions according to the type of attack

Crime Prevention Through Environmental Design (CPTED)

Crime prevention through environmental design involves effectively using the environment to observe intruders in order to reduce opportunities for crime and protect legitimate occupants. 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
- External environment surrounding the building

Natural access control

- Direct people and vehicles to specific access points
- Discourage or prevent access with physical or symbolic barriers (signs)

Reinforcing territories and defining boundaries

- Clearly distinguish public zones from private zones
- Create a sense of ownership for legitimate users and occupants
- Increase the vigilance of legitimate users in order to spot malicious parties
- Indicate to malicious parties 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

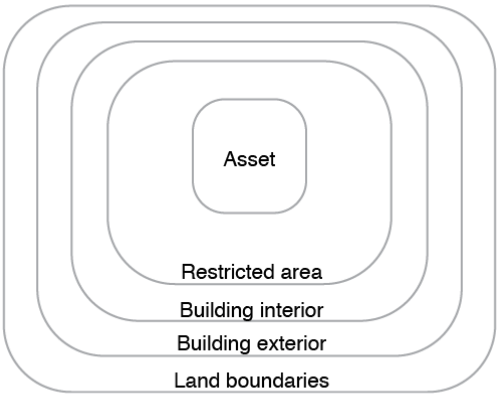
- Ensure premises are well maintained

Security lighting (interior/exterior)

- Overlap lighting to reduce unlit spaces
- Standardize lighting in all zones
- Limit glare

Defence-in-depth

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



Building envelope – protecting openings

Most building intrusions occur through doors and windows. If possible, openings should have a resistance equivalent to that of walls.

Types of openings:

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

- Company employees, visitors, and suppliers
- Some employees for certain sensitive areas (offices, computer rooms)
- At all hours or certain hours of the day or night
- To people, vehicles, and goods

Access control principles

- Minimize the number of entry points for easier access control
- Clearly mark entry points with an easily identified perimeter like a door or furniture arranged in a specific way
- Control access to all entry points to screen the people and materials that enter

Access control methods

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

Managing access rights

In order to ensure safe management of physical access points, access to a zone or asset should only be granted when required by a person's function, regardless of their hierarchical status.

Managing access devices

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

- Limit the number of access devices in circulation to a minimum
- Keep the devices in a locked cabinet and limit access to the people responsible for granting them
- In case of loss, theft, or compromise, recode locks and deactivate cards
- Maintain a log of access devices granted and in storage
- Periodically review the access devices issued
- Review access devices on termination of employment, at the end of a contract, or change of function

Managing visitors

Access control procedures must also be put in place for visitors. A visitor is a person who is not a company employee and must access a zone reserved for employees. The goal is to prevent visitors from accessing a restricted zone 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 at least 24 hours of protection in the case of a power outage
- Keep the number of alarm system users to a minimum
- Remove any users who are no longer needed when their employment is terminated
- Assign authority levels based on tasks to be performed

- Equip the alarm system with two modes of communication with the alarm control unit
- Conduct periodic testing of the alarm system
- Install sirens inside

Video surveillance

Video surveillance can be a valuable part of a company's security system. It is mainly used to:

- Detect activities that require a security response
- Collect images of an incident for further review and use as evidence, if necessary
- Help in assessing an incident

The functional requirements of a video surveillance system can be determined by answering these questions:

- What is the purpose of the system?
- What should each camera monitor?
- What are the requirements for real-time monitoring or the recording of images?
- What are the lighting constraints?

Video surveillance and privacy protection

Images and other information captured by a video surveillance system constitute personal information under the law. Because video surveillance is a form of invasion of privacy, certain obligations must be met concerning the collection and retention of personal information.

Advice for buying

Here are some important things to know when requesting a quote from a security service provider.

- Ask for a detailed quote (parts, labour, travel, annual fees, etc.)
- Ask for plans that show where components are located
- Purchase equipment that can be supported by several suppliers so you can switch suppliers without having to replace equipment
- Ask about service delays in case of a malfunction

Additional information

For more information, see:

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