WORKBOOK 11.2: SECURITY COUNTERMEASURE POLICIES AND PROCEDURES

Purpose: To provide information about selected security countermeasures that require policies and procedures

Section 1: Information about Perimeter Barriers

In addition to the standards for fences, there are standards that should be included in policies and procedures for perimeter barriers such as doors, windows, and other areas of the facility including but not limited to roofs, loading docks, public utilities, and air conditioning systems.

Standards for Doors

External doors	Install external doors made of solid hardwood, metal, solid laminated core, or solid multi-ply construction
	Strengthen solid softwood doors with a steel plate over the outer face of the door
	Configure external doors to open outwards
	Cover external door hinges to prevent pin removal
	Ensure doors are close-fitting and equipped with suitable locks
	Seal or protect letter receptacles and doors not in use
	Install locking bars across the back of the door
Glazed doors	Strengthen by adding a steel a mesh grille
Double doors	Fasten with bolts attached to the first closing leaf of the door and add a security deadlock
Interconnecting doors	Apply the same reinforcement technique as for external doors
Internal doors	Keep the keys for the locks secure
Emergency exit doors	Ensure compliance with local area fire regulations
Door frames	Strengthen the frame and its attachment to the building structure
Door bolts	Use door bolts in conjunction with security locks and fitted in pairs
	Ensure that bolts cannot be opened from outside the door
	Ensure that the bolt engages into the floor fully and the hole in the floor is kept free from obstruction

Standards for Windows

Windows	Brick up or otherwise secure all accessible nonessential windows
	Install secure fittings to all basements, ground floor, and other windows which are readily accessible
	Examine window catches and replace defective catches
	Consider providing intruder alarms for protection
	Identify responsibility for securing windows with potential access from ground floor level or reasonable climbing heights
	Ensure ground floor windows and those that are easily accessible to entry have locking handles or opening restrictors
	Consider installing bars, grilles, or shutters where necessary
	Consider installing intruder detection sensors
	Apply double glazing to provide additional protection against surreptitious or forcible attack

Standards for Other Areas

Grilles and shutters	Use expanding grille gates, roller grilles, or roller shutters in doorways, passages, or other openings
Roofs	Block access to facility rooftops by erecting suitable barriers, inserting grilles, and other potential entry points
	Install intruder alarms to detect unauthorized access
	Incorporate suitable measures to protect access to a building from attic or roof space
Skylights, fanlights, and roof lights	Replace the glass with security glazing material
	Fit the lights with bars or grilles
	Screw the frames in place and cover the glass with steel mesh
	Install an intruder detection system
Downpipes	Restrict access by boxing in the pipes or by treating them with anticlimb devices
Sunken outside areas	Secure steel grilles or steel mesh screens from below
	Fit vents into sunken areas or vents emerging at street level with internal steel grilles
	Install padlocked crossbars fitted on the inside to prevent access through service tunnels

	Install an intruder detection system
Loading docks	During business hours, use a custodian or electronically operated shutters so that the bay doors only open when an incoming vehicle is identified
	After business hours, close roller shutters or sliding shutters that secure from the inside
Public utilities	Install grating and intruder detection systems to block usage of cables and pipes entering the building
Air conditioning and other systems	Restrict access to provide adequate protection from sabotage
Multi-occupancy buildings	Ensure other tenant organizations secure their portion of the building at the same level as you
	Ensure that the security measures applied to your organization consider the existing tenant security levels

Section 2: Information about Closed-Circuit Television

Another type of policy and procedure to develop is for the use of closed-circuit television.

Benefits

- Saves manpower, especially when used in conjunction with an intruder detection system and automated access control system
- Supplements and extends, making an existing security system more effective
- Enhances the effectiveness of perimeter security particularly if used to verify the alarms signaled by perimeter intruder detection systems

Functions

- Assists with security personnel effectiveness
- Can be used to direct responses and assist in the control of incidents
- Deters intruders
- Assists in post-event analysis and incident investigation
- Assists with entry control
- Provides general operational information to aid in running the premises
- Provides site monitoring at night
- Can be fitted with video detection capability to monitor the external areas to the facility
- Can be used as a management tool for alarm verification

Image Requirements

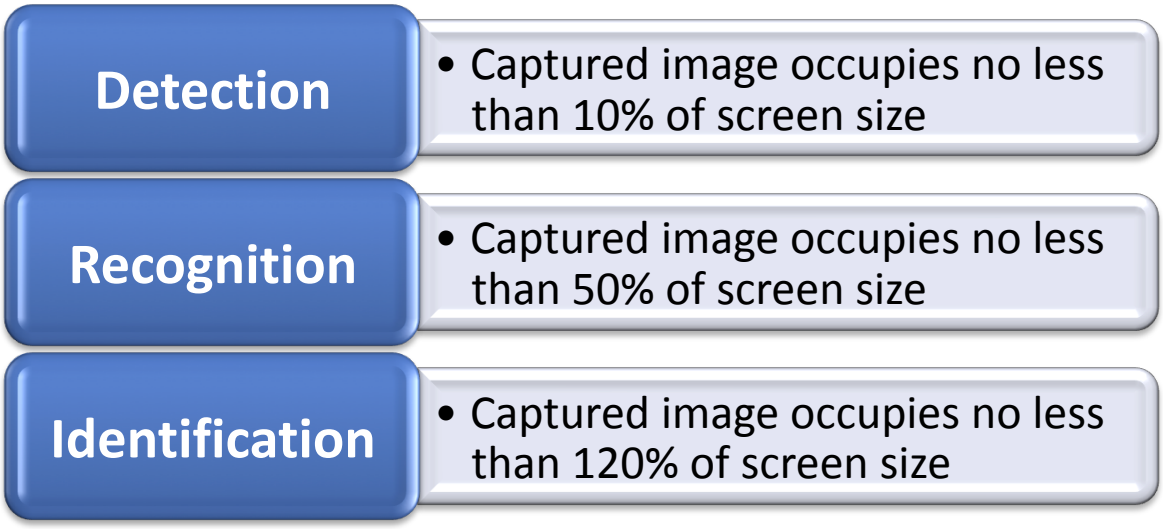

Image Standards

Closed-circuit television cameras should be an integral part of the physical protection system and deployed in areas where they achieve the following standards:

- Position closed-circuit television cameras so that you are able to monitor the main entrance for entry and exit surveillance **(identification)**.
- Use cameras at each external access control point and in conjunction with an intercom, if direct viewing of visitors is not possible **(identification)**.
- Support all access-controlled perimeter barriers with the use of intercom and closed-circuit television cameras **(recognition)**.
- Ensure closed-circuit television cameras provide surveillance of the facility perimeters with no gaps (**recognition**).
- Install closed-circuit television cameras so that you can view vehicle parking areas (**recognition**).
- Place closed-circuit television cameras to monitor the entrance and exit from critical areas and secondary areas (**identification**), including:
  - Facility back-up power systems
  - Security control center
  - Heating and ventilation supply
  - Switching rooms and build rooms (power supply rooms)
- Confirm that closed-circuit television cameras provide internal area surveillance (**recognition**).
- Ensure that the lighting is adequate and compatible with closed-circuit television cameras to ensure that they provide clear images (**detection**, **recognition**, **identification**).
- Verify that closed-circuit television systems are installed with video motion detection, where necessary (**detection**, **recognition**, **identification**).
- Monitor all installed and properly maintained closed-circuit television systems on a 24-hour a day, 7 days a week basis.

  - Ensure that an appropriately trained security force is available to respond to any identified alarms or incidents.
  - The system should be capable of being remotely monitored and recording should preferably be digital and be retained for a minimum of 30 days **(recognition and identification)**.
- Register the systems, where applicable, with the local law enforcement **(detection, recognition, identification)**.

Digital recording of closed-circuit television cameras is recommended and should meet the specification details established by the chief of security.

- Specific requirements will depend on the type of digital recorder to be installed, the cost appraisal for the number of cameras to be recorded on opening and the number of cameras likely to be used in the future.
- The digital recording system should be controlled by the chief of security.

Section 3: Information about Lock and Key Controls

Use the following guidelines when developing policies and procedures related to lock and key controls.

Standards

- Issue keys based on authorized employee and contractor identification system
- Keep the number of keys issued for any lock to a minimum
- Maintain a record (master key register developed by the local security force) showing the following:
  - The identifying features of each key such as the type registered, key number, and number of the duplicate
  - The identifying details of persons allowed access to each key
  - The date the working key (but not the duplicates) was signed out to the custodian
- Check the keys in at the end of each working day when used to directly protect sensitive environments; place unused keys in locked key boxes within the security control center
- Ensure that keys are not accessible to persons who do not have authorized access to the material or to the room (area) that the lock protects
- Do not remove security keys from the facility without the specific authority of the lead security officer
  - Treat in-use security keys with the same value and sensitivity as the material and environment they protect
  - Store, protect, and handle the keys accordingly
- Conduct periodic checks so to account for all keys
- Change keys and combinations when any of the following events occur:
  - Loss or compromise of keys
  - Suspected loss or compromise of keys
  - Termination of employment of any key holder
  - On a regular basis (for example, every 90 days)

Spare Keys

- Place spare keys to security locks in approved security containers by a designated member of staff
- Do not hold spare keys in the same container as the working key
- Issue a spare key only to persons with authorized access to the area or material the lock protects and only with documentation proving that the working key has been mislaid or lost
- Record the details of any spare keys that have been issued
- Supply additional keys only on the written authority of the lead security officer

Key Labeling

- Label keys to facilitate daily issue with clear markings and designated hook on key panel
- Do not identify the specific item the key opens:
  - Gate
  - Door
  - Container
- Check key rings or fobs frequently to ensure that keys cannot become detached. Note: a key fob is a type of security token. It is a small hardware device with built-in authentication mechanisms to control access to network services and information.