LOCKNET

PHYSICAL SECURITY AUDIT CHECKLIST

Security audits can encompass a wide array of areas; however, a cursory checklist is below:

Physical layout of the organization's buildings and surrounding perimeters:

- ☐ Does the property topography provide security or reduce the means of attack or access?
- ☐ Does the landscaping offer locations to hide or means of access to roof tops or other access points?
- ☐ How many points of entry are there to the building? Are those entrances monitored?
- ☐ Do all persons entering and exiting the building go through a security check point?

Lighting:

- ☐ Is there sufficient lighting to allow guards, employees, or others to see places of possible concealment or access?
- ☐ Are access points obscured by low light?

Alarms – including fire, intrusion, tamper, motion:

- ☐ Are doors, windows, gates, turnstiles monitored for egress and ingress?
- ☐ Are means of ingress able to be audited to identify who accessed those areas?
- ☐ Is the premises monitored for fire or smoke? Does the system alert the local fire department?
- ☐ In the event of a forced entry who does the alarms system notify? Is it monitored by a third party or staff?

Physical barriers – including fences, bollards, tire strips, gates:

- ☐ Are fences tall enough to reduce unauthorized access to the property? Is the fence checked regularly by staff for holes, damage or access points.
- ☐ Are bollards in place to prevent damage to buildings or access points by vehicles?
- ☐ Are tire strips installed and able to be used to prevent unauthorized entry to sensitive areas around the property? Parking lots, loading docks, pick up areas.
- ☐ Are gates secure and operating properly?
- ☐ Is entry to the premises protected by gates or is vehicular traffic allowed to move freely on and off the property?

LOCKNET

Access points – including doors, gates, turnstiles, windows, docks, elevators and stairwells:

- ☐ Are doors and gates in good working order? Do they operate properly and close on their own?
- ☐ Do turnstiles operate properly and are credentials required to go through?
- ☐ Are windows locked if they are able to be opened?
- ☐ If large panes of glass are installed in the building, are they laminated with a security film to prevent forced entry?
- ☐ Do docks and dock doors operate properly, and are they locked when not in use?
- ☐ Are elevators and stairwells checked for daily or hourly by security staff?

Guards:

- ☐ Does the organization's property utilize a guard staff?
- ☐ Do guards verify persons coming on the property are allowed access? How do they verify? ID, Verify with staff members, inspect vehicles, record names and license information?
- ☐ Do the guards make rounds on the property to check places of access? Doors, windows, elevators, stairwells, dock or bay doors, secured areas?
- ☐ Do guards complete check sheets while on duty to verify they checked as directed?
- ☐ Do guards vary their patrol patterns to reduce the chance of their routines being exploited?

CCTV:

- ☐ Are the perimeter of the building and the perimeter of the property adequately covered by cameras?
- ☐ Are cameras able to switch automatically from daytime to nighttime/low light?
- ☐ Are the building entrances and exits monitored by cameras?
- ☐ Are stairwells and other access points monitored by cameras?
- ☐ Are the cameras monitored 24 hours a day or only reviewed after an incident has taken place?

LOCKNET

Access methods – including locks, proximity cards/swipe cards, code or cipher locks, and other credentialing methods:

- ☐ Are locks and locking equipment in good repair and operating properly?
- ☐ Do past employees still have keys/access cards to the building?
- ☐ Have past employees/ terminated employees been removed from having access to the property?
- ☐ How often are codes changed on code or cipher locks?

Methods of communicating security breaches to the security staff or persons responsible for the organization's security. Including – local alarms/lighting, phone, text, email etc:

- ☐ How are security personnel notified of breaches in security and unauthorized access? Guards, local alarms, monitored alarms, phone calls?
- ☐ Does your security staff know the organization's policies for notifying management or other key personnel?