

Office Security Assessment

Completed by:

Location:

Description:

Survey Date:

Local Crime Statistics:

Describe the area and surrounding neighborhoods.

Insert crime statistics obtained from local Police Department

Type of Crime	2019	2020	2021
Assault			
Burglary			
Homicide			
Larceny			
Larceny from Motor Vehicle			
Robbery			
Sexual Assault			
Stolen Motor Vehicle			
Other			
Other			

If there have been any threats to employees or others in the last several years note this information here:

A.	Written Programs and Procedures	
	Is there a written Emergency Action Plan (EAP)?	
	Describe elements of the EAP in place.	
	Is there a Workplace Violence Prevention Program (WPVPP)?	
	Is there an Active Shooter Plan?	
	Are there procedures for lock-down?	
	Is there a public address system?	
	Does the facility have the ability to communicate to all employees?	
	Does the facility have the capability to communicate to all employees	
B.	Facility Inspected	
	Name	
	Address	
	Site representative	
	Position and title	
C.	General Information on Site	
	Building owner	
	Person in charge of security	
	Principal activities of facility	
	Occupancy Hours	
	Number of tenants	
	Are employees issued ID Badges?	
	Approximate number of daily visitors	
	Nature of surrounding area and occupancies (note security hazards)	
	Proximity to major roads and highways	
	Address and telephone number of police jurisdiction	
	Are local crime statistics available and for what period?	
	Is there a business-community-based crime prevention program in place? Of what does it consist?	
	Are outside power transformers and other utilities properly secured?	
D.	Site Perimeter	
1.	Bus terminals, train stations close by?	
2.	Total area of site	
3.	Landscaping	
	What is the landscaping?	
	Are there natural barriers present?	

D.	Site Perimeter <i>(continued)</i>	
	Is shrubbery well pruned so as not to provide concealed hiding places?	
4.	Is there a perimeter barrier?	
5.	Parking	
	Is there public parking and/or metered parking directly adjacent to the building?	
	Are signs posted to make the public aware of vehicle towing policies?	
	Is the perimeter patrolled?	
6.	Perimeter Lighting	
	Types of perimeter lights	
	Does lighting minimum local codes?	
	Lights directed toward the perimeter?	
	Are all exterior doorways, walkways, and entries properly illuminated?	
	Dark areas where criminals may conceal themselves?	
	What additional lighting is required to illuminate these areas?	
	Is lighting on an automatic timer?	
	Lights in operation throughout night?	
	Exterior lighting protected against theft and vandalism?	
	Lighting system regularly inspected? By whom?	
	Is there an emergency lighting system in the event of a power failure?	
7.	Exterior Cameras	
	Is video surveillance used?	
	Are cameras black & white or color?	
	Are cameras analog or digital?	
	Are outside cameras weatherproof?	
	Do cameras need to be added?	
	Who monitors the cameras?	
	Are cameras monitored remotely?	
	Is video recorded?	
	If recorded, for how long?	
E.	Parking Areas	
	Is there a parking structure?	
	Are there weight restrictions?	
	Is there a gate to the facility?	
	How is access to the area controlled?	
	Is there a private parking lot?	
	Is the area public or private?	
	Who operates the facility?	
	Number of entrances and exits?	
	Do trees obstruct view of structure?	

E.	Parking Areas <i>(continued)</i>	
	Is shrubbery well-pruned to protect against concealed hiding places?	
	Designated parking areas for tenants?	
	Is there assigned visitor parking?	
	Is use of designated spaces enforces?	
	Are executive names on spaces?	
	Number of parking spaces	
	Is vehicle access controlled?	
	Are there speed bumps in the lot?	
	Is a speed limit sign posted?	
F.	Building	
1.	Construction	
	Building height, number of floors	
	Total square footage	
	Typical floor size	
	Construction type	
	Year of construction	
	Are there atriums or mezzanines?	
2.	Entrances, Doors and Reception	
	Construction of doors	
	Number of entrances	
	Do all employees and visitors enter by one primary entrance?	
	Are all entrances monitored?	
	Is the main entrance monitored?	
	Are doors self-closing?	
	Do doors self-lock?	
	Do exterior doors have the ability to lock remotely?	
	Do interior doors have the ability to lock remotely?	
	Is there a reception area?	
	Is it monitored during working hours?	
	Is the reception area separated from the office workspace?	
	Is the reception area locked?	
	Are guests escorted through the facility?	
3.	HVAC	
	Are heating, ventilating, and air conditioning (HVAC) system intakes accessible from outside the building?	
	How is the HVAC system protected?	
4.	Windows	
	Are ground floor windows protected?	
5.	Stairwells	
	Number of stairwells & configuration	

F.	Building <i>(continued)</i>	
	Are stairwell doors self-closing and self-latching?	
6.	Restrooms	
	Are there public restrooms?	
	Are public restrooms kept locked?	
	If so, who controls access?	
	Can restroom doors be locked from inside?	
7.	Rooftop	
	Is access to building possible from adjacent roofs?	
	Is it possible to access the building from the roof?	
	Is there a helipad or heliport?	
8.	Lighting	
	Is the lighting of the building interior adequate?	
	Is lighting adequate in corridors, exits, and stairwells?	
	Is there an emergency lighting system for power failures?	
9.	Intrusion Alarm Systems	
	Are alarm systems installed?	
	What type(s) are they?	
	How are alarms monitored?	
	Who monitors these alarms?	
	Can the system be viewed remotely?	
	What is the procedure when an alarm is received?	
	Whose responsibility is it to switch the alarm system off and on?	
	Does leaving alarmed doors open defeat the security system?	
	Are duress/panic alarms used?	
	How frequently are alarms tested?	
	Are there up to date lists of personnel authorized to open and close alarmed areas?	

F.	Building <i>(continued)</i>	
	Are intrusion detection, video surveillance, and access control systems properly maintained (and equipment problems documented)?	
	Are the security alarm, video surveillance, and access control systems inspected and tested on a regular basis (and this documented)?	
10.	Access Control	
	Is there access control for parking?	
	Is there access control into building?	
	Are there sign-in/sign-out logs?	
	Are visitors issued an ID badge?	
	Are visitors escorted in the building?	
	Are vendors issued an ID badge?	
	Are ID badges readily distinguished?	
11.	Electronic Key Card Systems	
	Are electronic key card systems used?	
	What vendor is utilized?	
	Are all doors on the key card system?	
	Are systems properly maintained (and equipment problems documented)?	
	Are systems inspected and tested on a regular basis (and this documented)?	
12.	Video Cameras	
	Is video surveillance used?	
	Are cameras black & white or color?	
	Are cameras analog or digital?	
	Do cameras need to be added?	
	Who monitors the cameras?	
	Are cameras monitored remotely?	
	Is video recorded? And for how long?	
	How long are images kept?	
G.	Key Control	
	Who is in charge of key control?	
	How many master keys are in existence and who has these?	
	Is there documentation of which employees have master keys?	
	Is there a record of key issuance?	
	How are keys tracked for each employee?	
	Are employees required to notify HR if a key lost or stolen?	
	What are the security measures for key boxes?	

G.	Key Control <i>(continued)</i>	
	Describe the control system. Is the system adequate?	
	What is the frequency of record and key inspections?	
	Are locks immediately replaced when keys are lost?	
H.	Office Computers	
	Computers permanently identified and inventoried?	
	High-value items physically secured?	
	Are desktop personal computers anchored using devices?	
	Are desktop computers, laptop, and notebook computers kept locked up?	
	Are passwords used to limit access?	
	Are data files backed up daily?	
	Are copies of data backups, program backups, and forms kept offsite?	
	Are there physical security measures to protect the workstations and the file server?	
	Is privacy of user-ID and passwords maintained?	
	Is a trusted, well-trained individual in charge of controlling access to programs and data?	
	Are compromises of the systems immediately and thoroughly investigated?	
	Does the office have local area network (LAN) and wide area network (WAN) systems?	
	Is access to this area tightly controlled? How is it controlled?	
	Is a trusted, well-trained individual in charge of controlling access to programs and data?	
	Are back-up records made of sensitive information, with copies stored on and offsite?	
	Is there a separation of staff working on system development and system operations?	

I.	Janitorial Services	
	Who is responsible for the janitorial operation?	
	Are outside contract or building in-house employees used?	
	Are their backgrounds checked?	
	What are the hours of operation?	
	How are janitorial staff supervised?	
	Are janitorial staff required to wear a distinctive uniform and photo ID cards?	
	Is the supervision adequate of the staff?	
	Do they possess keys?	
	How are keys controlled?	
	Are transparent trash bags used?	
	Are spot checks made of the contents of trash bags?	
	Is trash temporarily stored at the site?	
	How long is it stored?	
	Is the trash placed in a dumpster, compactor, etc.?	
	How is trash removed from the site?	
	Are boxed and cartons flattened before removal?	
	Is trash removal supervised? By whom?	
	Are janitorial staff permitted to use stairwells?	
	Where do they take meal and rest breaks?	
	Are they permitted to go to their private vehicles during breaks?	
	Are janitorial supplies kept properly secured?	
	Does janitorial equipment being used always remain in the building?	
	Are janitorial staff trained in security awareness?	
	Are janitorial supervisors informed in a timely manner of theft activity occurring in tenant areas?	
	Are janitorial staff searched and/or their personal belongings checked when they leave the site?	

Security Assessment Form developed by: Hettrick, Cyr & Associates