April 2017
Interim Revision January 2021
Page 1 of 31

SUPERVISION OF PROPERTY

Table of Contents

Page

List of Figures

List of Tables

1.0 SCOPE

This data sheet covers property supervision and its relationship to loss prevention and mitigation. Included are recommendations and information on preventing unauthorized access to both premises and assets, including information technology networks, industrial controls networks, and alarm services for both security and fire that can mitigate property loss and business interruption, including cyber risk.

For protection against burglary and theft, see Data Sheet 9-16, *Burglary and Theft.* Note: The recommendations on passive building protection in this data sheet (9-1) take precedence over those in Data Sheet 9-16.

For protection against incendiary fires see Data Sheet 10-6, *Protection Against Arson and Other Incendiary Fires.* Note: The recommendations in this data sheet (9-1) take precedence over those on protection of “all properties” in Section 2.2.1, Data Sheet 10-6.

For information on the prevention of freeze losses see Data Sheet 9-18, *Prevention of Freeze-Ups.*

For detailed information on fire alarms and fire detection systems, refer to Data Sheet 5-40, *Fire Alarm Systems,* and Data Sheet 5-48, *Automatic Fire Detection.*

1.1 Hazards

Inadequate security can result in unauthorized access to a facility or a facility’s critical assets (including communication networks such as information technology networks and industrial controls networks), which may lead to damage or loss of property and an interruption of normal business activities. Assessing and categorizing the consequences of viable threats, including cyber risks, are vital steps in creating a security program, without which the necessary measures to eliminate or mitigate those threats cannot be taken. Also, if alarm systems are not provided or monitored correctly, an incident (e.g., fire, intrusion) could worsen before being noticed.

1.2 Changes

January 2021. Interim revision. Editorial updates were made to provide clarity on recommendations.

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

The goals of property supervision are to deter, detect, and/or delay unauthorized access, and alert the proper authorities about other hazards, such as fire. This document provides general guidance on the subject; each facility must evaluate their own specific property supervision needs via a physical security risk assessment and use the results to develop a security program and a physical security incident response plan.

Use FM Approved equipment, materials, and services whenever they are applicable and available. For a list of products and services that are FM Approved, see the *Approval Guide,* an online resource of FM Approvals.

2.2 Human Element

2.2.1 Security Program

Create a written security program based on a physical security risk assessment and a facility security map. Ensure the plan addresses all of the security risks associated with the facility. Security programs are best developed by teams. Varied perspectives and backgrounds ensure all hazards and threats are recognized. Ensure the security program is aligned with emergency response, disaster, and business recovery plans.

2.2.1.1 Physical Security Risk Assessment

The scope of the physical security risk assessment will depend on many factors, including facility size, occupancy, and processes. The scale of the physical security risk assessment can range from a simple assessment conducted by a qualified team of employees to a complex assessment by a certified third-party consultant.

A security vulnerability assessment (SVA) that meets the recommendations in this section and the guidelines established by the organizations listed in Section 3.1.1.1 can be used to fulfill the recommendation of a physical security risk assessment.

A well-developed physical security risk assessment typically includes the steps and processes recommended below.

2.2.1.1.1 Define the organization and facility to be protected.

A. Define critical assets.

B. Determine the effects of losing these critical assets.

2.2.1.1.2 Perform a vulnerability analysis. Identify the actual and potential threat scenarios and determine a security risk level for each critical asset.

2.2.1.1.3 Develop security measures. Identify physical and procedural security options that could prevent or mitigate threats.

2.2.1.1.4 Assess risk reduction. Enhance security measures based on the risk of those measures being compromised. The following are some factors to consider:

A. Reduced probability of successful unauthorized access

B. Degree of risk reduction provide by the security measures

C. Feasibility of the security measures

D. Capability and effectiveness of the security measures

E. Reliability and maintainability of the security measures

F. Cost of the security measures

2.2.1.1.5 Consider the risk of unauthorized access in regard to the following facility infrastructure elements:

A. Locations/site

B. Building and structures

1. Envelope

2. Interior

C. Information technology networks

D. Industrial control networks (Operational Technology - OT)

E. Utility systems

1. Mechanical

2. Plumbing

3. Electrical

F. Fire alarm systems

G. Security systems

H. Equipment operation and maintenance

2.2.1.1.6 A formal report by the physical security risk assessment provider should document the findings and recommendations. Use this document for review, tracking, and management.

2.2.1.1.7 Review (and consider re-conducting) the physical security risk assessment at the following times:

A. After a significant security incident has taken place (as identified by the security manager or the manager of the facility)

B. When a threat substantially changes (as identified by the security manager or the manager of the facility)

C. When it is proposed that an existing building construction feature, area, process, or operation be substantially changed

D. Periodically, to revalidate the assessment

2.2.1.2 Facility Security Mapping

2.2.1.2.1 Map the facility into areas of various security levels and designate each area as one of the following (or similar designations that meet the same intent):

A. **Unsecured-Open** (employees and visitors allowed)

B. **Unsecured-Protected** (employees and screened visitors allowed)

C. **Secured-Controlled** (screened visitors allowed if accompanied by an authorized employee)

D. **Secured-Restricted** (no visitors and only authorized employees allowed)

2.2.1.2.2 Factors to consider when mapping an area of a facility include, but are not limited to, the following:

A. Sensitivity and criticality of the operation

B. Interior area vulnerability to damage, interruption, alteration, or other harm

C. Sensitivity and value of the information or property stored within or at the interior area

D. Location of the area in the occupancy and vulnerability to intrusion

E. Intended accessibility of the area (e.g., public, shared use)

F. Egress for personnel safety

2.2.2. Security Program Development

Develop a written security program. At a minimum the plan should do the following:

A. Designate a member of management to supervise the plan, review surveillance reports daily, investigate irregularities such as missed tours or tour stations, and institute changes as necessary to maintain the integrity of the plan.

B. Identify the responsible party to check for conditions that may cause a fire, security breach, or other loss.

C. Identify all areas of the facility that are unoccupied during operating and non-operating hours.

D. Identify procedures to be followed by security personnel or the party responsible for reporting specific incidents (i.e., which conditions require immediate action or can simply be reported to management according to routine schedules).

E. Include the facility security map created in Section 2.2.1.2.

2.2.2.1 Employee Access

In accordance with the security program, implement procedures to control employee access to both the building and restricted areas within the building. Include the following as applicable:

A. Provide employee identification/security badges to every employee. In accordance with the security program, implement one of the following rules:

1. Employees display their identification/security badges at all times.
2. Employees display their identification/security badges on demand.

B. Use security personnel or identification/security badge readers at doors to various areas of the facility based on their security designations.

C. Prohibit “tailgating” or “piggybacking” (i.e., holding doors open for visitors, contractors, or other employees) at doors that require security badges.

D. Provide training on the company’s security program to all employees.

E. If an employee's role changes, evaluate the need to modify that employee's security access.

F. Upon employee termination, revoke access to the facility (i.e., ensure terminated employees return their identification/security badges, parking permits, etc.).

2.2.2.2 Visitor Access

In accordance with the security program, implement procedures to control visitor access to both the building and restricted areas within the building. Include the following as applicable:

A. Document all incoming and outgoing visitors.

B. Screen all visitors (for proper identification, company credentials, etc.) who enter the property or building.

C. Use visitor identification/security badges to control and monitor access to the building. In accordance with the security program, implement one of the following rules:

1. Visitors display their identification/security badges at all times.
2. Visitors display their identification/security badges on demand.

D. Provide identification/security badges to control access to areas inside the building. In accordance with the security program, implement one or both of the following rules:

1. Visitors can be given identification/security badges to access unsecured-protected areas.
2. Visitors must be escorted in secured-controlled areas.

2.2.2.3 Contractor Access

2.2.2.3.1 Adhere to the appropriate recommendations in Data Sheet 10-4, *Contractor Management.*

2.2.2.3.2 In accordance with the security program, implement procedures to control contractor access to both the facility and restricted areas within the facility. Include the following as applicable:

A. Document all incoming and outgoing contractors.

B. Screen all contractors (for proper identification, company credentials, etc.) who enter the property or building.

C. Use contractor identification/security badges to control and monitor access to the facility. In accordance with the security program, implement one of the following rules:

1. Contractors display their identification/security badges at all times.
2. Contractors display their identification/security badges on demand.

D. Provide identification/security badges to control access to areas inside the building. In accordance with the security program, implement one or both of the following rules:

1. Contractors can be given identification/security badges to access unsecured-protected areas.
2. Contractors must be escorted in secured-controlled areas.

E. Provide all contractors with a security briefing and explanation of the security program. Preferably, include the security program in the contract for the work.

F. Have short-term contractors (see Appendix A for definition) supervised while they are working on the property.

G. Have contractors escorted during non-business hours.

2.2.2.3.3 Provide a method and procedures to ensure contractors using computers or other portable media (USB drives) to service equipment do not introduce a cyber risk (e.g., malware, viruses) to the information technology network.

2.2.2.4 Facility Securement Procedure

In accordance with the security program, implement a facility securement procedure for non-business hours. Include the following as applicable:

A. Lock all perimeter gates and other pedestrian access points.

B. Lock all doors to the exterior of the building and interior areas that are designated as secured and restricted.

C. Lock all windows to the exterior of the building.

D. Set all monitoring and alarm security systems.

E. Limit the access of after-hours contractors to a single, controlled entrance to the property and building.

F. Create a securement checklist and update it annually or whenever relevant changes are made.

2.2.2.5 Key-Control Procedures and Records

In accordance with the security program, implement a key-control procedure. Include the following as applicable:

A. Rekey locks when a key to an area designated as unsecured-protected, secured-controlled, or secured-restricted (or equivalent designation) is lost.

B. Maintain access lists for people authorized to draw master keys.

C. Secure key storage containers and cabinets.

D. Perform security checks of key storage containers and cabinets.

E. Perform an inventory of keys annually (or at a frequency in accordance with the security program).

F. Maintain a written record of key issuance requests, approvals, and issuances.

G. Destroy or secure keys that have not been issued or are no longer needed.

H. Discretely identify keys or key tags by use of a coding system.

I. Train employees on key-control policy and procedures.

J. Maintain key-control records that include the following information:

1. Number assigned to each key and lock
2. Location of each lock (room number, industrial control equipment or IT cabinet) by unique identifier
3. Person to whom each key has been issued
4. Date of issuance
5. Date of return
6. Documented acceptance for each key issued and returned

2.2.2.6 Physical Security Incident Response Plan

2.2.2.6.1 Create and implement a physical security incident response plan to be followed when unauthorized access of various kinds has been detected. Include the following in the plan:

A. Define the events to be considered incidents that warrant a response.

B. Define roles and responsibilities and how facility personnel should respond under various circumstances, including contacting outside authorities or resources.

C. List the facility’s incident reporting requirements. Have all incidents documented and reviewed by management.

2.2.2.6.2 Include procedures for responding to the following incidents, as applicable:

A. People who forget or lose access cards

B. Visitors/vendors/contractors who cannot verify a reason for entering, or when an inside contact cannot be reached to approve their entrance

C. Suspicious activity witnessed at the guard entrance, on video surveillance, or during other screening processes

D. Unauthorized access to the property (e.g., over a wall, forced entrance through a gate)

E. Unauthorized access to the production network

F. Unauthorized drone activity in the vicinity or directly over the property

2.2.3 Security Program Implementation and Training

2.2.3.1 Security Management

Designate a person to oversee the security program and be responsible for the following as applicable:

A. Training security personnel or employees responsible for security

B. Monitoring security training (to ensure security personnel are following procedures)

C. Running training programs associated with the security program and implementing the physical security incident response plan.

2.2.3.2 Awareness Training

Provide on-going physical security awareness training to employees. Ensure employees are familiar with the facility's culture on physical security and the protocols established to prevent unauthorized access to the facility and restricted areas.

2.2.3.3 Practice Drills

2.2.3.3.1 Perform periodic practice drills simulating unauthorized access to the facility and fire incidents at various times and locations. (See Section 3.2.2.)

2.2.3.3.2 Document the results of practice drills and review them with management for plan effectiveness and possible improvements.

2.2.3.4 Audits

Audit and update the security program annually to address changes.

2.2.4 Security Functions

2.2.4.1 Have the following security functions performed (by employees, an outside security service, or a combination of both), as applicable. Ensure the functions are in line with the security program and are audited regularly.

A. Identification and control of employee, visitor, and contractor movement on the property.

B. Identification and control of vehicular movement on the property.

C. Coordination and communication with management, ERT or fire service, and law enforcement.

D. Surveillance of security hazards and critical assets by recorded tours. Video monitoring from a constantly attended location that is used as an integral part of a security system is considered a supplement rather than a replacement for recorded tours.

E. Surveillance of arson hazards and ignition sources. For example: checking for discarded smoking materials, combustible trash properly disposed, yard storage, heat sources turned off or down when possible, unneeded electrical circuits de-energized, and unattended continuous operations involving heat or chemical reactions.

F. Checking areas where hot work has been performed at the proper frequency in accordance with FM Loss Prevention Data Sheet 10-3, *Hot Work Management.*

G. When appropriate, visually check fire protection equipment to confirm its readiness in an emergency. This could include the following items:

1. Visually check sprinkler control valves to confirm they remain secure and are in the open position.
2. Confirm fire pumps have adequate fuel (if appropriate) and remain in the automatic start mode.

3. Check water level and temperature in fire protection water storage tanks.

4. Check air pressure in dry-pipe sprinkler systems.

5. Check temperature in heated dry-pipe valve enclosures.

H. Check passive security devices (doors, gates) and active security systems (alarms, video surveillance) for functionality and operability.

I. Act as alternate positions within the emergency response team (ERT) when ERT members are not available. The duties of an ERT will vary from facility to facility. Refer to Data Sheet 10-1, *Pre-Incident Planning,* for detailed guidance on emergency response team responsibilities.

J. Provide additional security tours or surveillance in areas that are not constantly attended.

K. Provide additional or extended security tours at facilities during holidays, weather emergencies, or annual operational shutdowns.

2.2.4.2 Properly locate tour stations, if used, to ensure security personnel pass through the full length of all major areas of the facility. Electronic surveillance can be used to supplement actual tours but they should not replace them entirely if the security program calls for them.

2.2.4.3 Provide security personnel with a fast and reliable method of communication with management and the ERT or fire service.

2.2.4.4 Vacant, Strike-Bound, or Idle Properties

When properties are vacant, strike-bound, idle, or experiencing reductions in the work force, do the following:

A. Provide a minimum of one recorded visit to the facility per week.

B. Provide property supervision as recommended in Data Sheet 10-6, *Protection Against Arson and Other Incendiary Fires.*

2.3 Equipment and Processes

2.3.1 Property Access

2.3.1.1 Control access to the property in accordance with the security program. Include the following as applicable:

A. Perimeter Barriers

1. Perimeter barriers should consist of fences and/or walls, plus gates as needed for access. In some cases, the perimeter barrier should be contiguous around the entire facility. Design the barrier to resist entry using hand tools, such as by spreading the bars of a fence to provide an opening. Ensure fences have sufficient support to resist overturning by manual force.

2. Ensure the perimeter barrier has sufficient space between potential horizontal footholds or is designed with other anti-climb measures.

3. Use metal fences of heavy industrial-grade construction with bars spaced closely together. Chain-link fences and gates should not be used. Walls should be reinforced masonry or concrete construction.

4. Provide gates of the same or similar design and materials as the adjacent fences. Gates may be access-card operated from the outside or as prescribed by the security program.

5. Arrange pedestrian and bicycle gates to swing in the outward direction.

6. Preferably, vehicular security gates should be sliding or cantilevered and only wide enough to accommodate one vehicle lane. The vehicular gates should be capable of being locked.

7. Arrange physical barriers to also protect cooling equipment, generators, fuel tanks, and utilities.

8. Where anti-ram rated vehicle barriers are needed, select active or passive barriers based on the appropriateness of the architecture of the facility and the specifics of the site and natural environment.

B. Guards/Gate Houses

1. When included in the security program, perimeter entrances for pedestrians and vehicles should be provided with enclosed guard houses for personnel, gate operation, vehicle inspection, and information.

2. Design guard houses to permit the guard to perform duties from within the guard house. Provide the guard house with a secondary means of egress.

3. Provide guard houses with power, telephone, intercom, data, and other equipment as needed.

4. If needed, design guard houses to be ballistic-resistant (doors, walls, and windows), and protect guard houses with bollards.

C. Parking and Vehicle-Screening Areas

1. Locate parking away from the building.

2. Ensure vehicles belonging to employees, contractors, guards, and cleaning crews display parking permits.

3. For contractors entering the site, verify there are established contracts in place and that individuals have been pre-screened and approved, if necessary, for entrance.

4. Vehicles with no permits, including visitors, should be parked in visitor parking areas.

5. Provide separate entrances to the site for external visitors and employees of the facility. When separation of types of traffic is not feasible, use card-controlled access gates and other traffic separation measures.

6. Establish a screening area with adequate space and site utilities to accomplish the following tasks, as appropriate:

a. Visual identity check of driver’s identification.

b. Visual inspection of vehicle interior, including luggage compartment, cargo boxes, and trailers.

c. Trace element swipes and sensors.

d. Confiscation of phones, tablets, recording devices, etc.

D. Protective lighting that is continuous in the following areas:

1. Entry/egress points

2. Pedestrian/bicycle pathways

3. Vehicle routes

4. Parking structures and lots

5. Signage

6. Loading areas

7. Yard storage

8. Trash collection areas

9. Building utility services (e.g., transformers, emergency generators)

10. Areas under video surveillance

E. Protection for exterior utility supplies (water, communications, gas, electricity, etc.) against vandalism and unauthorized access

1. Use perimeter barriers as appropriate.

2. In critical occupancies, have these areas monitored by constant personnel surveillance, surveillance systems at constantly attended locations, or with an alarm system.

2.3.1.2 Where access to the perimeter of the property will be secured, provide the following in accordance with the security program:

A. Exterior Lighting

1. Illuminate an area on either side of perimeter barriers in accordance with the security program.

2. Provide illumination sufficient to enhance trees, landscaping, and buildings without dark shadowy areas that may compromise security

3. Mount lights on the roof or poles so they are not easily disabled.

4. If exterior video surveillance is provided:

a. design lighting to facilitate proper camera function.

b. use sufficient or redundant security lighting such that enough lighting is available should any light fail.

B. Intrusion alarm systems

1. Provide an intrusion alarm system if the security program indicates a need for one.

2. If an intrusion alarm system will be provided, select an appropriate level system (see Data Sheet 9-16, *Burglary and Theft*).

C. Access control systems (e.g., locks, turnstiles)

D. Video surveillance systems

1. Provide surveillance at high risk points outside the building:

- Entry and exit points
- Parking lots
- Neighboring property
- Yard storage
- Garbage bins
- Power and cooling facilities

2.3.2 Building Access

2.3.2.1 Control access to buildings in accordance with the security program. Include the following as applicable:

A. An access control system to identify visitors and contractors and prevent unauthorized personnel from entering unsecured-protected, secured-controlled, and secured-restricted areas.

B. The minimum number of entry/egress points for safe and efficient operation of services and in accordance with local codes.

C. Exterior doors that have the following features:

1. Substantial construction with adequate locking devices as follows:

a. A metal facing or solid metal door.

b. In accordance with the occupancy-specific data sheet

2. Windows with force-resistant glazing or that are protected by metal grill work.

3. The door frame should also be of substantial construction, well secured to the structure.

4. A heavy dead-bolt lock should be provided, with a bolt that extends at least 1 in. into the bolt receptacle.

5. Hinges that are tamper-proof from the exterior.

D. Do not use locks that require electrical power, e.g. electromagnetic locks, to secure physical access.

E. Secure access control to the building with the following:

1. lock(s) or electronic key systems

2. automatic closing and securely latching entry/egress points

F. Windows that are located and/or constructed to help prevent unauthorized access. For example, located so they are visible from main roads and not easily reached from the ground or nearby structures, and/or constructed using tempered or wired glass or steel bars. See Section 3.3.4.

G. Security tour stations at outside access points to the building and to interior areas containing critical assets.

H. Continuous lighting at all access points to the building and areas under video surveillance.

1. Illuminate areas around building entrances.

2. Mount lights on the roof or poles so they are not easily disabled.

3. If exterior video surveillance is provided, do the following:

a. Provide lighting to facilitate proper camera function.

b. Use sufficient or redundant security lighting that enough lighting would still be available should any one light fail.

I. The minimum number of openings/penetrations on the building exterior (walls, roof, and underground utility and personnel tunnels) for facility operation, and in accordance with local codes.

1. Keep openings usually closed.

2. Have critical openings monitored by constant personnel surveillance, surveillance systems at constantly attended locations, or with an alarm system.

3. Protect openings larger than 12 in. (0.3 m) with tamper-proof grills.il

J. Protection from unauthorized access and vandalism for exterior equipment (e.g., emergency generators) and HVAC penetrations.

1. Secure openings in air-handling systems.

2. Protect exterior equipment in accordance with Section 2.3.1

3. In critical occupancies, monitor exterior equipment and openings by constant personnel surveillance, surveillance systems at constantly attended locations, or with an alarm system.

K. Skylights, if installed, protected with a security grill.

L. The minimum number of vehicle access openings necessary for normal operation. Openings should be regularly closed and locked and/or monitored by surveillance systems.

M. Authorized emergency response team (ERT) personnel that are provided with access (e.g., master keys, passcodes) to equipment areas protected by locks so they can gain access in the event of a fire.

N. An intrusion alarm system if the security program indicates a need for one. If an intrusion alarm system will be provided, select an appropriate level system (see Data Sheet 9-16, *Burglary and Theft*).

O. Video surveillance systems, if installed, provide the capability for complete coverage of the perimeter of the building, roof access points, and exterior equipment.

2.3.3 Interior Access

2.3.3.1 Control access to interior areas of buildings in accordance with the security program. Include the following as applicable:

A. An access control system with personnel identity verification to allow only authorized personnel to enter.

B. The minimum number of entry/egress points for safe and efficient operation of services.

1. Ensure all entry/egress points are highly visible.

2. Do not post signs identifying high-value rooms and areas.

3. Provide physical access controls so only one visitor at a time is allowed to enter into any secured-controlled area.

4. If applicable, provide a fire-rated door in accordance with the recommendations in the occupancy-specific data sheet.

C. Access secured with the following:

1. Lock(s) or electronic key systems

2. Automatic closing and securely latching entry/egress points

2.3.3.2 Provide authorized emergency response team (ERT) personnel with access (e.g., master keys, passcodes) to equipment areas protected by locks so they can gain access in the event of a fire.

2.3.3.3 Have walls constructed from the floor deck to the ceiling deck.

2.3.3.4 Provide limited interior windows. When installed, provide tempered or wired glass for windows.

2.3.3.5 Provide continuous protective lighting at the following places:

A. Entry/egress points

B. Areas under video surveillance

C. Within secured areas (provide lighting that is either continuous or automatic upon detection of motion)

2.3.3.6 Secure openings in air-handling systems. When an opening exceeds 96 in^2 (620 cm^2), protect the opening with physical devices (e.g., steel bars, grills, wire mesh, or fencing).

2.3.3.7 Where security systems are to be installed, provide the following in accordance with the security program (see Section 3.3.6, Security Systems):

A. Intrusion alarm systems

1. Provide an intrusion alarm system if the security program indicates a need for one.

2. If an intrusion alarm system will be provided, select an appropriate level system (see Data Sheet 9-16, *Burglary and Theft*).

B. Access control systems

C. Video surveillance systems

2.3.3.8 If the shipping and receiving area of a building is to be secured, do the following in accordance with the security program:

A. Provide an area for screening and authorization of shipments into the facility.

B. Ensure shipments being received are identified with corresponding purchase orders or requisitions.

C. Do not accept undocumented deliveries.

D. Inspect packages for tampering or damage. Report any damaged or suspicious packages to the carrier.

E. Document and track receipt of hazardous materials.

F. Have couriers entering the building identified in accordance with Section 2.2.2.2, Visitor Access.

2.3.4 Confidential Document Access

2.3.4.1 Establish a procedure and provide a method for physical destruction of confidential paper documents that no longer need to be retained (e.g., shredders or secure bins for contracted shredding service).

2.3.5 Information and Operational Technology Network Access

2.3.5.1 In accordance with the security program, secure access to equipment rooms or closets in which communication or information system cabling is routed. These areas include data processing equipment rooms, server rooms, wiring closets, etc.

2.3.5.1.1 Do not use signage to identify these high-value rooms and areas.

2.3.5.1.2 If these high-value areas have suspended ceilings or raised floors, construct the walls from the floor deck to the ceiling deck, and seal the openings.

2.3.5.2 Do not locate circuits and cables in public areas. If unavoidable, limit access by providing the following:

A. Circuits and cables in conduit

B. Junction boxes that can be closed and fastened

2.3.5.3 If internet access is needed or desired for visitors, provide password-protected access to an independent “guest” Wi-Fi network with internet access only (i.e., does not provide access to internal production and/or business networks). Change the password frequently and provide it only on request (i.e., don’t make it publicly available).

2.3.5.4 Provide safeguards to prevent unauthorized physical access to electronic assets (e.g., computers, process control systems, production network) to avert damage or loss of data. Provide the following in accordance with the level of security indicated in the security program:

A. Provide an automatic, timed (no more than 15 minutes) lock-out of computers and mobile devices when left unattended for which a password is used to regain access.

B. Control connection of unauthorized computers to the production network from Ethernet ports/outlets. This could mean physically controlling access to the ports (e.g., cover plates) or some kind of network access control (e.g., the network does not recognize unauthorized devices).

C. Do not locate Ethernet ports/outlets that connect to the production network in public areas.

D. When located in unsecured areas or co-locations, provide locks on server rack doors to prevent access to connection and cable ports (see Figure 1).

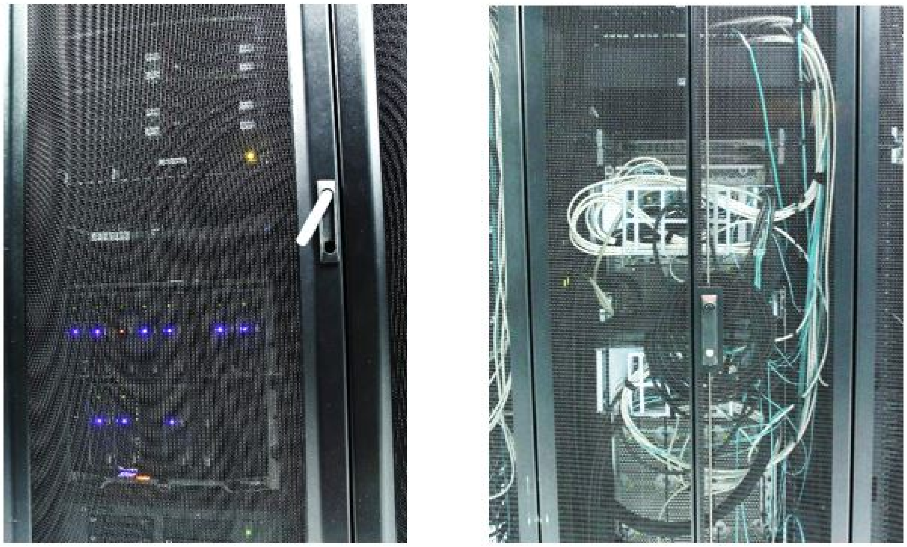


Fig. 1. Front and rear of server racks with locks

E. Use special types of screws to secure servers to racks (e.g., Allen screws rather than standard screws).

2.3.5.6 When unauthorized physical access to the network is detected, ensure the appropriate response is covered in the physical security incident response plan (see Section 2.2.2.6).

2.3.5.7 Establish a procedure and provide a method for physical destruction, secure wipe (i.e., not standard disk formatting), and/or degaussing of data storage devices (e.g., traditional hard disk drives and solid-state drives found in computers, copy machines or other equipment) that are no longer in service. Refer to Section 3.3.6.4, Sanitization of Hard Drives, for guidelines on media sanitization.

2.3.6 Fire Protection

2.3.6.1 Assign a member of the emergency response team (ERT) who is present during operating hours to be a “notifier” in accordance with Data Sheet 10-1, *Pre-Incident Planning.*

A. Train the notifier to report a fire to the fire service in accordance with Data Sheet 10-1, *Pre-Incident Planning.*

B. During non-operating hours, have the notifier function performed by trained security personnel in accordance with Data Sheet 10-1, *Pre-Incident Planning.*

2.3.6.2 Provide local waterflow, fire-pump running, and trouble alarms with a reliable response at properties meeting either of the following criteria:

A. All areas are constantly occupied by employees 24 hours per day, 365 days per year.

B. Adequate security service is provided, making recorded tours when the property is not in operation or is less than fully occupied.

2.3.6.3 At properties not meeting the criteria in Section 2.3.6.2, provide a minimum Class V level of alarm service (see Appendix C).

2.3.6.4 Where other fire protection features (fire pumps, smoke detectors, special protection systems, etc.) are also monitored, connect the electrically supervised alarm signals to the fire service, municipal dispatch center, FM Approved proprietary system, or FM Approved central station.

2.3.6.5 Throughout all areas of combustible construction or occupancy, provide one of the following:

A. FM Approved heat, smoke, or flame detection (as appropriate) with supervised alarm transmission to an FM Approved central station, proprietary system, or constantly attended public fire service.

B. Supervised waterflow alarm transmission to an FM Approved central station (FM Approved where available), proprietary system, or constantly attended public fire service (Class V, see Appendix C), if automatic sprinkler protection is provided.

C. Security service conducting hourly recorded tours. If this option is selected, protect concealed spaces of combustible construction or occupancy with a supervised fire detection system or sprinkler system.

2.3.6.6 Protect properties prone to or having experienced incendiary fires in accordance with Data Sheet 10-6, *Protection Against Arson and Other Incendiary Fires.*

2.3.7 Physical Security Systems

2.3.7.1 Install physical security systems in accordance with Data Sheet 9-16, *Burglary and Theft,* and the manufacturer’s specifications.

2.3.7.2 In addition, for video surveillance systems, provide the following:

1. Integrate motion detection with the video surveillance system to automatically monitor, process, and record information.

2. Locate the video monitors in a constantly attended area.

3. Protect video cameras from vandalism.

4. Store video surveillance footage on site for at least 90 days or the maximum allowable time in accordance with governing codes, standards, and laws. Transfer recordings to back-up media and store in a dry, cool, central location that is secure.

5. Conduct video recording in real time using a digital video recorder (DVR), network video recorder (NVR), or a time-lapse video recorder (VCR).

6. Protect video recording equipment from vandalism and theft.

7. Have video recordings secured both on site and at a remote location.

8. Use intelligent video analytics to identify objects left behind, count people, and employ other “smart” tactics to quickly spot real threats.

2.4 Operation and Maintenance

2.4.1 Test and maintain all security and fire protection equipment in accordance with the applicable data sheet and the manufacturer's recommendations.

2.4.2 Repair or replace all security and fire protection equipment on a priority basis in accordance with the security program.

A. Maintain a document that lists repairs, including the following:

1. The impairment to the device, equipment, or system
2. The time and date of the impairment
3. Repairs that were completed
4. The time and date of each repair

B. Maintain the repair document for not less than 1 year.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Human Element

3.1.1 Physical Security Risk Assessment

A physical security risk assessment is intended to evaluate the current vulnerabilities of a facility relative to unauthorized access and related threats. The extent of the assessment is dependent upon an organization's size, resources, and capabilities. The physical security risk assessment is a vital first step in determining the level of supervision and security a facility requires in its security plan. At a minimum, it is vital to know the answers to the following questions:

A. What needs to be protected?

B. Why does it need to be protected?

C. How can it be protected?

D. What is the likelihood of that protection being breeched?

3.1.1.1 Security Vulnerability Assessment (SVA) Providers

The following organizations have members that are certified security professionals:

A. Physical Security

American Society for Industrial Security (ASIS) International
Worldwide Headquarters: Alexandria, VA, USA
236 Chapters worldwide
www.asisonline.org/Pages/default.aspx

International Association of Professional Security Consultants (IAPSC)
575 Market Street, Suite 2125
San Francisco, CA 94105
www.iapsc.org

B. Information Technology Networks

ISACA International Headquarters
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008
www.isaca.org

www.isaca.org/CERTIFICATION

(Previously know as Information Systems Audit and Control Association)

(ISC)^2 Corporate
311 Park Place Blvd

Suite 400
Clearwater, FL 33759
www.isc2.org/

www.isc2.org/credentials

SVA templates are provided on some of these organizations webpages for reference.

The following documents provide information on conducting risk assessments and security vulnerability assessments:

American Petroleum Institute (API). *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries.*

American Society for Industrial Security (ASIS) International. *General Security Risk Assessment Guideline.*

American Society for Industrial Security (ASIS) International. *Facilities Physical Security Measures. ASIS GDL FPSM.*

American Society for Industrial Security (ASIS) International. *Risk Assessment. ANSI/ASIS/RIMS RA.1.*

Federal Risk and Authorization Management Program (FedRAMP). *Security Assessment Report (SAR) Template.*

International Standards Organization (ISO) / International Electrotechnical Commission (IEC). *Information technology - Security techniques - Information security management systems - Requirements.* ISO/IEC 27001.

National Institute of Building Sciences Task Group. *Physical Security Assessment for Department of Veterans Affairs Facilities.*

National Institute of Standards and Technology Special Publication 800-30, *Guide for Conducting Risk* Assessments.

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing Security Controls in Federal Information Systems.*

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers.*

SafePlace Corporation. *SafePlace Security Vulnerability Assessment Workbook.*

3.1.1.3 SVA Costs

The typical cost for a security vulnerability assessment when conducted by a consultant will vary based upon the type, size, and complexity of the occupancy. Typical costs are as follows:

A. Office Building

- Time on site: 2 days
- Assessment, report development: 1 week
- Approximate cost: US$5000

B. Intermediate Manufacturing Facility

- Time on site: 3 to 4 days
- Assessment, report development: 1 to 2 weeks
- Approximate cost: US$5000 to US$10,000

C. Chemical Plant

- Time on site: 1 week
- Assessment, report development: 1 month
- Approximate cost: US$20,000

3.1.2 Contractor Access

Contractors and third-party providers who require access to the organization’s production network should be provided with the ability to access only those specific systems, applications, and/or network segments required to perform their contracted responsibilities. Where feasible, restrictions should be in place to limit contractors’ and third-party providers’ ability to copy, paste, or download information from remote systems, applications, or network devices.

3.1.3 Property Supervision

Good property supervision is usually achieved when all of the following are true:

A. Well-trained and concerned employees are in constant attendance (24 hours per day, 365 days per year).

B. 100% of the facility is occupied at least once per hour.

C. Local alarms can be heard by employees.

D. An adequate emergency response team is provided.

If a facility is in continuous operation but there are some areas that are unattended for several hours or more per day, additional supervision may be needed for those areas. The fact that a facility is in continuous operation does not, by itself, satisfy the need for supervision. If unattended areas (1) are visited hourly by security personnel or members of the emergency response team, or (2) have alarms that can be heard by personnel in attended areas, or (3) have detectors/alarms connected to a constantly attended area, no additional supervision is needed if the emergency response team and/or security personnel are adequate on all shifts and can respond promptly.

During normal operating periods where the majority of areas are occupied, reliable emergency response team response to fires, unauthorized access to the facility, and other hazards is usually ensured. If security service is to be omitted, there is still a need for some supervision. At locations where it is determined that security service is not needed, an employee (preferably a member of the emergency response team) should make a thorough tour of the property at the end of the day or at the end of each shift.

When operations are to be shut down for an extended period, such as during vacations or holidays, several precautions can be taken to limit the possibility of loss. These include removing combustible waste, storing ignitable liquids properly, shutting off ignitable liquids or flammable gas mains, and making a thorough inspection of the property. If freezing temperatures are anticipated, sufficient heat must be maintained in the building to prevent freezing of automatic sprinkler piping, domestic water piping, and process equipment and piping.

The frequency of loss is often greater at vacant or idle properties. Therefore, there should be no reduction in the level of supervision provided at such properties. In addition, it is important to maintain the aesthetic condition of the property.

Studies have shown that properties allowed to deteriorate (e.g., broken windows, unkempt landscape) are more prone to unauthorized access, vandalism, and arson than well-kept properties in the same neighborhood. During times of emergency, such as impairments to the fire protection system, loss of the alarm system, loss of electrical services, flood, hurricane, labor disputes, riot, civil disorder, or the aftermath of a tornado or earthquake, security service is vitally important. In these instances, alarms and automatic supervision are not sufficient since they may be out of service or subject to a delayed response. Even when security is normally provided, in these instances it is usually necessary to increase the number of security personnel and the frequency of tours. Additionally, when emergency conditions are imminent, the security force can be augmented with personnel capable of making temporary repairs to the building envelope, to fire protection systems, and to equipment vital to production or mitigation of the loss.

3.1.4 Management Responsibilities

Whether security is provided by a third party (contractor) or by employees of the company, senior management retains the responsibility for providing adequate property supervision. It is particularly risky to rely on the generic practices and procedures of a security firm. The security program must be tailored to the individual property in order to obtain the level of effectiveness required. The development of security practices and procedures must be a collaborative effort between production, facilities, and risk management in order to provide a comprehensive plan that considers the unique hazards associated with the property.

3.1.5 Frequency of Security Tours

Frequency of tours will depend on the size of the property, occupancy, values, importance of the processes, activity in the area, etc. Below are general guidelines:

A. In general, have tours performed hourly in unoccupied areas and twice-hourly during normal business hours unless indicated otherwise in specific recommendations.

B. Have security tours begin within one half hour after an area becomes unoccupied and continue to no more than one half hour before an area will be reoccupied.

C. Where video surveillance and other types of electronic surveillance are used, tour frequency can be reduced to at least one tour per shift.

3.1.6 Supervisory Systems and Communication

There are two types of guard tour patrol systems:

A. Remote supervision. Stations are located throughout the property that are electronically connected to a proprietary system at a constantly attended location or to an outside central station.

B. Local supervision. This method consists of a data collection unit carried by a security guard. When each station is visited, the unit records the location and time.

Each system has its advantages and disadvantages. The use of a data collection unit provides flexibility in both the ability to move the stations easily and add stations as needed, while remote supervision by a central station often requires the guard to maintain a strict routine. Tours must be started and each station reached within a certain amount of time and at a specific time. This dictates a pattern that may increase susceptibility to organized burglaries or theft.

Supervision by an FM Approved central station or proprietary system, however, does provide the following additional benefits: (a) back-up for security personnel in the event of accident, sudden illness, burglary, or hold-up; (b) emergency service in the event security personnel become incapacitated; (c) prompt discovery of delinquencies of the security staff; and (d) a convenient method of summoning the fire service. These extra benefits are especially valuable when a few security personnel are the only people on the property.

Communication has a direct bearing on the efficiency with which security personnel can operate. Security guards must be able to communicate with supervisors and management routinely. Telephone communication is a viable option if the property is relatively compact. Often when operations cease for the day, or at normal shutdowns, only a few telephones remain active for incoming and/or outgoing calls. If this is the case, it must be verified that active telephones are available along tour routes. A combination of telephone and radio communication is preferred. Hand-held two-way radios provide increased mobility and reliability when emergencies (e.g., hurricanes, tornadoes, floods) affect electrical power and telephone lines. Cellular telephones can be used in lieu of radios; however, their reliability is somewhat less since they rely on transmission and relay towers or dishes that can be affected by the same storms causing the emergency.

Paging systems and public address systems are generally not suited for security communications. Paging systems rely on the guard to use a telephone to respond, and public address systems are only one-way communication and are not secure since anyone in the area can hear the message.

3.2 Training

3.2.1 Initial Training

Initial training is vitally important. An unsupervised security officer must never be assigned to duty without first being trained in the specific hazards, alarm systems, protection systems, and protocols of a facility, and given a tour of the property. Good training includes the following:

A. Discussion of and procedures associated with the site-specific emergency and security programs (i.e., SIRP).

B. Discussion of building identification (names, numbers, etc.)

C. Building occupancies

D. Description of and procedures associated with special hazards

E. Layout and operation of fixed automatic fire protection systems

F. Layout and operation of manual and portable fire protection equipment

G. Details on intrusion alarm and fire detection systems

H. Emergency shutdown procedures for equipment and processes

International, national and industry standards can be used to define roles, capacities and training of security personnel if it meets the intent of this standard.

On-going training is also important since production processes and facility occupancies change frequently and rapidly in some industries. The security staff must be kept current on hazards associated with production. Changes in any of the above items will have an impact on the security program and duties of the security staff.

3.2.2 Practice Drills

These can be walk-through or table-top drills in which unauthorized access is simulated for different breaches of security and fire incident scenarios, including various severity levels.

3.3 Physical Security

A critical aspect of property supervision is preventing unauthorized access to the property, building envelope, and secure areas within the facility. Once a physical security risk assessment has been completed, a site-specific security program can be developed to coincide with the results of that assessment. The physical devices and safeguards implemented will vary depending on the goal (limiting unauthorized property access, building access, or interior access), as described in the following sections.

Other passive factors, such as site location, physical barriers, landscaping, lighting, vehicle screening, and parking locations contribute to the overall security of the site perimeter. Simply providing an initial point of control at the perimeter of the property or the outermost level of the facility provides a heightened level of security.

3.3.1 Physical Barriers

Physical barriers used in conjunction with motion detection sensors, video surveillance cameras, and motion-activated lighting can serve as an effective first means of defense against intrusion. Where it may not be possible to install heavy-duty fencing, gates, or barriers, there are options such as sensors and network camera-based technologies that can be used to compliment basic physical barriers or create virtual barriers at the perimeter of a property.

3.3.2 Lighting

3.3.2.1 Lighting can be important to the effectiveness of a security system by augmenting physical barriers, intrusion detection systems, video surveillance, and security personnel activities. Where exterior security lighting is to be installed, the following types can be provided in accordance with the security vulnerability assessment and the security program:

A. Continuous: illumination devices installed in a series to maintain uniform lighting during hours of darkness.

B. Glare projection; deters potential intruders by making it difficult to see into an area.

C. Standby: illumination devices are not on continuously but are turned on:

1. Automatically at random intervals or by intrusion detection systems

2. Manually at random intervals or when suspicious activity is suspected by security personnel

D. Controlled: illumination devices cover a limited space with little spill over into other areas.

E. Emergency: illumination devices that may be a duplicate for any of the previous systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. An alternate source of power should be used for operation.

F. Portable: illumination devices that are manually operated and moveable that may be lit during darkness to as needed.

3.3.2.2 The following types of security lighting can also be provided in accordance with the security vulnerability assessment and the security program:

A. Streetlight: Projects a downward circular illumination pattern.

B. Searchlight: Projects a very narrow high-intensity beam of light to concentrate on a specific area or item.

C. Floodlight: Projects a medium to wide beam on a larger area. It is used in a variety of settings, including perimeters of commercial, industrial and residential areas.

D. Fresnel: Projects a narrow, horizontal beam. Unlike a floodlight, which illuminates a large area, the fresnel can be used to illuminate potential intruders while leaving security personnel concealed. It is often used at the perimeters of industrial sites.

E. High mast lighting: Projects a wide beam on a large area. This is utilized mainly in parking lots and along roads and usually varies in height from 70 to 150 feet (20 to 46 m).

F. Infrared: Projects electromagnetic energy that is not visible to the naked eye, but is useful for video surveillance illumination.

3.3.2.3 The lighting source or lamp of lighting equipment have specific characteristics related to color rendition, intensity (lux or foot-candles), life span, and start up times. Those characteristics need to be evaluated with the type of equipment and application it is being used. As examples:

A. mercury vapor light sources take several minutes to produce full light out put so would not be appropriate for standby applications, but would be appropriate for continuous lighting.

B. Video surveillance systems typically dictate the proper level of lighting intensity for minimum function and maximum performance. Image quality is also affected by excessive shadows (light to dark ratio), lens glare, and backlighting. A low pressure sodium light source provide poor color rendition as compared to a metal halide light source which provides accurate color rendition.

3.3.3 Landscaping

Landscaping features such as trees, bushes, boulders, etc., can hide the building from passing cars, obscure security devices (such as fences), and also help keep vehicles from getting too close.

3.3.4 Windows

Where the security program calls for securing windows, various types of window glass and protection methods can be provided. Ensure the types and methods used do not conflict with the applicable building and fire codes.

A. The following are various types of window glass that could be used:

1. Tempered glass: Treated to resist breakage. Building codes may require tempered glass for safety reasons (when it breaks, it forms small pieces rather than shards).

2. Wired glass: Provides resistance to large objects, but may still shatter. Typically used in doors to maintain fire rating.

3. Laminated glass: Composed of two sheets of ordinary glass bonded to a middle layer or layers of plastic sheeting material. When stressed or struck, it may crack and break, but pieces of glass tend to adhere to the plastic material. For laminated glass to be effective it should be installed in a frame, and the frame secured to the structure.

4. Bullet-resistant or burglar-resistant glass: Provides stronger resistance to attack. Consists of multiple plies of glass, polycarbonate, and other plastic films laminated together to provide ballistic resistance.

B. Other window protection methods include the following:

1. Window bars: Steel bars can protect the window opening from being used as an access point. Specifications on the installation of window bars are provided in Data Sheet 9-16, *Burglary and Theft.*

2. Window film (fragment-retention film): Film that adheres to the interior of the surface of the glass, strengthens and holds the glass in place if broken.

3. Security shutters: Typically either a roll-up type, with horizontal interlocking slats that roll up into a box located at the top of the window; or an accordion type, with vertical interlocking slats that slide to the side of the window.

3.3.5 Interior Access

Where suspended ceilings or raised floors are present and security from unauthorized access is recommended to an area, installation of floor deck to ceiling deck wall construction will prevent access from the ceiling plenum or concealed space.

3.3.6 Security Systems

Table 1 lists various types of security systems and equipment that can be provided in accordance with the security program.

Table 1. Types of Security Systems

Intrusion Detection Systems	• Position detection devices • Motion detectors • Sound detectors • Vibration sensors • Heat sensors • Temperature sensors • Capacitance devices • Impact sensorsGlass break sensors • Duress/panic alarms
Access Control Systems	• Mechanical locks • Electrified locks • Electromagnetic locks • Credentialoperated locks • Turnstiles • Circlelock turnstiles • Biometric locks
Video Surveillance Systems	• Remote IP based network • IoT network • Close Circuit television

3.3.6.1 Intrusion Detection Systems

An intrusion detection system can identify and alarm unauthorized entry into protected spaces. Exterior sensors may include microwave sensors, infrared sensors, fence mounted sensors, or video motion detection.

3.3.6.2 Access Control Systems

3.3.6.2.1 A comprehensive access control system is designed to do the following:

A. Permit only authorized persons and vehicles to enter and exit

B. Detect and prevent the entry of contraband material

C. Detect and prevent unauthorized removal of valuable assets, including data

D. Provide information to security officers to facilitate assessment and response

Access control system can be manual, machine-aided manual, or automated. Manual systems (e.g., locks and keys, turnstiles) use personnel to control who or what may enter the facility. Machine-aided manual system use tools, such as metal detectors, to aid personnel in the access decision. Automated access control systems use technology to control the entire access process.

There are some inherent disadvantages in using mechanical keys and locks as the access control system: There is no record of the key being used on a specific door, keys can be copied or transferred to an unauthorized person, and keys do not restrict the key holder to specific times of access.

Automatic access control systems typically include a control device, reader, controller, and security barrier. The access control device is recognized by the reader. The reader sends the device identification to a controller. The “intelligence” of the reader may be classified as to the function it is expected to perform. If the controller makes the decision to allow access, it sends a signal to the ingress/egress point to open.

Part of the controller is comprised of security software that has a database as an integral component to control access. Database management requires special consideration because it needs to be continually updated by authorized persons to reflect employee status within the facility. In addition, the database may track visitor access passes and assign a time period for their use. It may be appropriate to periodically check the access history for attempts to gain entry to areas where the access card holder is not authorized to go, especially during unusual hours. Access to the database should be strictly limited. A system transaction history should be maintained and available for review.

3.3.6.2.2 In the design of the access control system, certain features need to be considered, including the following:

A. Whether the access control system will be integrated with other building systems, such as alarms, video surveillance, and elevators

B. Whether various components of the access control system will operate together effectively

C. Whether these systems will be actively monitored by professional security personnel or a trained employee

D. Ability of the access control system to disable access upon termination of an employee or loss of the key.

3.3.6.3 Video Surveillance

A perimeter video surveillance system can detect potential threats and intruders. For example, motion detection technology can trigger alarms. Video content analytics (VCA) can identify objects left behind, count people, and employ other “smart” tactics to quickly spot real threats. These technological advancements make the video surveillance system more responsive to potential security breaches because activity in the perimeter layer can be quickly assessed.

Consideration should also be given to the cabling infrastructure. IP-based video is delivered through the network in real-time, typically using User Datagram Protocol (UDP), which is the transmission of data from one node on the network to another, and is not guaranteed. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system such as video. Therefore, it’s critical that the physical layer systems, such as the cabling infrastructure, not cause transmission errors on the network.

3.3.6.4 Sanitization of Hard Drives

The National Institute for Standards and Technology’s (NIST) Special Publication 800-88: *Guidelines for Media Sanitization,* identifies preferred methodologies for sanitizing hard drives and other media.

3.4 Operation and Maintenance

Procedures and preventive maintenance should be implemented for maintaining fire protection and security systems. This is critical to ensure protection and security systems operate as intended during an emergency. The use of maintenance contracts is one method of ensuring the proper evaluation of operation on a regular schedule.

For lighting equipment, the following operation and maintenance inspections should be considered:

A. Check electrical circuits and test all connections.

B. Ensure proper lamp functionality.

C. Ensure lamps are kept clean and maintain their proper lighting angle.

D. Ensure the lighting intensity continues to meet security requirements (i.e., for video surveillance systems).

E. Ensure batteries are charged for emergency lighting in compliance with local codes.

3.5 Loss Experience

3.5.1 Illustrative Losses

3.5.1.1 Vandalism and Arson at a Data Center

A contract employee cut wires to computers and started a fire at an air traffic control center, damaging 23 of the 29 computers at the facility. Thousands of flights were delayed or cancelled as a result, and it took three days for normal operations to resume. The damage was such that a new air traffic control center had to be built at an adjacent facility.

3.5.1.2 Files Deleted from a Production Network

At an electrical systems integrator and custom metal enclosure manufacturer, an unknown person deleted numerous files from several different servers on the production network. The files were on file share servers, email servers, SQL servers, and domain controllers. This event had a significant negative impact on operations in multiple departments and three locations as it affected e-mail, access to files, and the VPN (remote employees could not access any of the systems).

3.5.1.3 Insider Threat

At a computer manufacturer, an employee tampered with a program involved in benchmarking the specifications for a very valuable proprietary computer system. The company spent a great deal of time trying to determine the cause of the difficulties they were experiencing. Finally, thinking the issues might be related to the room in which the testing was being performed, the entire project was relocated to another facility. The employee was later found accessing another employee’s computer, was confronted by management, and finally confessed to causing the problems. By that time, however, several million dollars had been spent and a lot of time had been wasted trying to resolve the problems.

3.5.1.4 Unauthorized Access at a Warehouse Storing Computer Components

At a warehouse that stored computer components, security guards were stationed at gate shacks on the exterior of the property 24 hours a day. An alarm activated and the security guards made an external sweep of the building, but did not observe any activity and decided the alarm was accidental. The perpetrators, meanwhile, made their way to the office area by cutting a hole in the sheet rock wall and then entered a valid code to disarm the alarm system. A torch was used to cut through the frame of the locking device on a gate, allowing entry to a high-value product cage. A box truck was driven into the warehouse through a ramp door and loaded with three pallets of computer CPU chips.

Following the loss, video surveillance showed four individuals breaking into the warehouse through a window in an unused breakroom.

4.0 REFERENCES

4.1 FM

Data Sheet 5-40, *Fire Alarm Systems*
Data Sheet 5-48, *Automatic Fire Detection*
Data Sheet 9-16, *Burglary and Theft*
Data Sheet 10-1, *Pre-Incident Planning*
Data Sheet 10-3, *Hot Work Management*

Data Sheet 10-4, *Contractor Management*
Data Sheet 10-6, *Protection Against Arson and Other Incendiary Fires*
Data Sheet 9-18, *Prevention of Freeze-ups*

FM Hot Work Permit System (P9104)

4.2 Other

American Petroleum Institute (API). *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries.*

American Society for Industrial Security (ASIS) International. *General Security Risk Assessment Guideline.*

American Society for Industrial Security (ASIS) International. *Facilities Physical Security Measures.* ASIS GDL FPSM.

American Society for Industrial Security (ASIS) International. *Risk Assessment.* ANSI/ASIS/RIMS RA.1.

Federal Risk and Authorization Management Program (FedRAMP). *Security Assessment Report (SAR) Template.*

International Standards Organization (ISO), International Electrotechnical Commission (IEC). *Information technology - Security techniques - Information security management systems - Requirements.* ISO/IEC 27001.

National Fire Protection Association (NFPA). *National Fire Alarm Code.* NFPA 72.

National Institute of Building Sciences (NIBS) Task Group. *Physical Security Assessment for Department of Veterans Affairs Facilities.* September 2002.

National Institute of Standards and Technology (NIST). Special Publication 800-30, *Guide for Conducting Risk Assessments,* September 2012.

National Institute of Standards and Technology (NIST). Special Publication 800-53A, *Guide for Assessing Security Controls in Federal Information Systems,* December 2014.

National Institute of Standards and Technology (NIST). Special Publication 800-88, *Guidelines for Media Sanitization,* September 2012.

National Institute of Standards and Technology (NIST). Special Publication 800-100, *Information Security Handbook: A Guide for Managers,* October 2006.

SafePlace Corporation. *SafePlace Security Vulnerability Assessment Workbook.* 2003.

APPENDIX A GLOSSARY OF TERMS

Access control: The control of persons, vehicles, and materials through the implementation of security measures.

Co-location: Rental to third parties of disk space, provision of web-hosting services on a server, or segmented facilities with various tenants who control their own equipment.

FM Approved: Products and services that have satisfied the criteria for FM Approval. Refer to the *Approval Guide,* an online resource of FM Approvals, for a complete listing of products and services that are FM Approved.

Guest access: Password-protected access with segmentation to a part of a facility's information technology system network (as opposed to unrestricted access).

Guest network: A secured segmented portion of a facility's information technology network set up for visitors, business associates, etc. to access the internet without access to the production network.

In-house contracted services: Personnel hired from an outside company to perform full-time job functions at the facility (e.g., a designated, in-house building engineer or security guard). Typically, contractors in this category would be granted access privileges similar to those of a regular employee.

Key: A physical device with incisions or electronically encrypted device that will operate a particular lock or sets of locks to open or close.

Long-term contractors: Personnel hired to perform work onsite for an extended period of time, usually relating to a renovation or construction project. These are contractors who may be onsite for several months or more. They may be granted office or storage space at the facility or may have an onsite portable office trailer.

Production network: A private and secured information technology network that a company uses to conduct their business transactions.

Risk Assessment: A process of identifying internal and external security threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical function necessary to continue operations, defining the controls in place or necessary to reduce the exposure.

Secured-controlled: An area or a level of security in which screened visitors are allowed only if they are accompanied by an authorized employee.

Secured-restricted: An area or a level of security in which no visitors and only authorized employees are allowed.

Security vulnerability assessment (SVA): A systematic and methodical analysis in which an occupancy's security vulnerabilities are identified, quantified, and prioritized to prevent and undesired outcome.

Short-term contractors: Personnel hired to perform work onsite in a temporary, short-term, or as-needed capacity, and who do not normally have security access to the facility. These contractors may be onsite for one day or several weeks.

Unsecured-open: An area or a level of security in which both employees and unscreened visitors are allowed.

Unsecured-protected: An area or a level of security in which employees and screened visitors are allowed.

APPENDIX B DOCUMENT REVISION HISTORY

The purpose of this appendix is to capture the changes that were made to this document each time it was published. Please note that section numbers refer specifically to those in the version published on the date shown (i.e., the section numbers are not always the same from version to version).

January 2021. Interim revision. Editorial updates were made to provide clarity on recommendations.

October 2019. Interim revision. Editorial updates were made with the issuance of Property Loss Prevention Data Sheet 7-110, *Industrial Control Systems*.

October 2017. Interim revision. Minor editorial corrections were made.

April 2017. This entire document has been revised. Major changes include the following:

A. Revised the scope of the document to include physical security recommendations and information that can minimize property loss and business interruption.

B. Added a description of the hazards associated with unauthorized access to a facility.

C. Added Section 2.2.1, Security Program, which includes recommendations related to performing physical security risk assessments and facility security mapping.

D. Added Section 2.2.2, Security Program Development.

E. Added Section 2.2.3, Security Program Implementation and Training.

F. Section 2.2.4, Security Functions.

G. Added Section 2.3, Equipment and Processes, which includes recommendations regarding the following:

- Property access
- Building access
- Interior access
- Confidential document access
- Information technology network access
- Fire protection

- Physical security systems

H. Added Section 2.4, Operation and Maintenance, which provides recommendations on adequate installation and maintenance of access alarms.

I. Added Section 3.1, Human Element, to support recommendations in the following areas:

- Physical security risk assessment
- Security vulnerability assessment (SVA) providers
- Risk assessment and SVA references
- SVA costs

J. Added Section 3.3, Physical Security, to support recommendations in the following areas:

- Physical barriers
- Lighting
- Landscaping
- Windows
- Interior access
- Security systems

K. Added Section 3.5, Loss Experience.

L. Updated Appendix A, Glossary of Terms, to include terms associated with the revised scope of this data sheet.

April 2012. Terminology related to ignitable liquids has been revised to provide increased clarity and consistency with regard to FM Global's loss prevention recommendations for ignitable liquid hazards.

May 2007. Appendix C was revised to include FM Global Fire Alarm Service classifications. In addition, some editorial changes were made.

September 2005. Revisions to this document are primarily editorial in nature. Also, the reference to Basic Protection and Managed Protection for non-HPR location supervision has been eliminated.

January 2000. This revision of the document has been reorganized to provide a consistent format.

APPENDIX C FM FIRE ALARM SERVICE CLASSIFICATIONS

Depending upon the size and value of the property, its operating hours, attended vs. unattended areas, and the presence or lack of security personnel, facilities can be protected by various classes of protective signaling systems or alarm service. The NFPA fire alarm classification system defined in ANSI/NFPA 72, *National Fire Alarm Code,* differs from the FM classification system. FM's system is used only for FM field application. The NFPA system is used by signaling system manufacturers and installers. It is also used to evaluate equipment during FM Approval examinations.

The FM fire alarm service classifications account for system reliability and expected response to the alarm. The information provided below will describe the FM class levels to assist in field application and define the supervision level at the premises.

C.1 No Waterflow Alarm, No Response

Locations with automatic sprinkler systems are normally equipped with at least a local waterflow alarm. The operation of sprinklers cannot be detected unless someone actually in attendance notices water is flowing. Without a waterflow alarm, response is uncertain and unreliable.

C.2 Class II: Local Waterflow Alarms, Unreliable Response

Class II alarm service means that local sprinkler waterflow alarms are provided at a location where response is uncertain, but where it can be expected to be noticed by someone if it activates for a long period of time. Response is uncertain when it depends on a chance passerby, a security guard on two- or three-hourly rounds, nearby residents, or personnel in other, often noisy facility areas, and connection to a fire alarm control that is unreliable or not FM Approved. Dependence on prompt notification being given to the proper authorities by untrained persons is also uncertain.

C.3 Class III: Local Waterflow Alarms, Reliable Response

Class III alarm service means local sprinkler waterflow alarms are electrically connected to an FM Approved fire alarm control provided at a location where reliable response is ensured. Reliable response means the alarms are located where the alarm indicator LED can be seen and the audible alert to the alarm can be heard by properly instructed personnel in constantly attended work areas, such as a boiler house, an all-night switchboard, a gate house, or a guard headquarters. Care should be taken to determine whether or not the waterflow alarms can actually be heard by the people who are expected to respond. Often, bells located on the outside walls can be heard inside the building only in their close proximity. Also, the person expected to respond should be a plant employee or some other person who has been instructed in the proper actions to be taken.

C.4 Class IV: Nonstandard Service, Waterflow Alarms, Unreliable Response

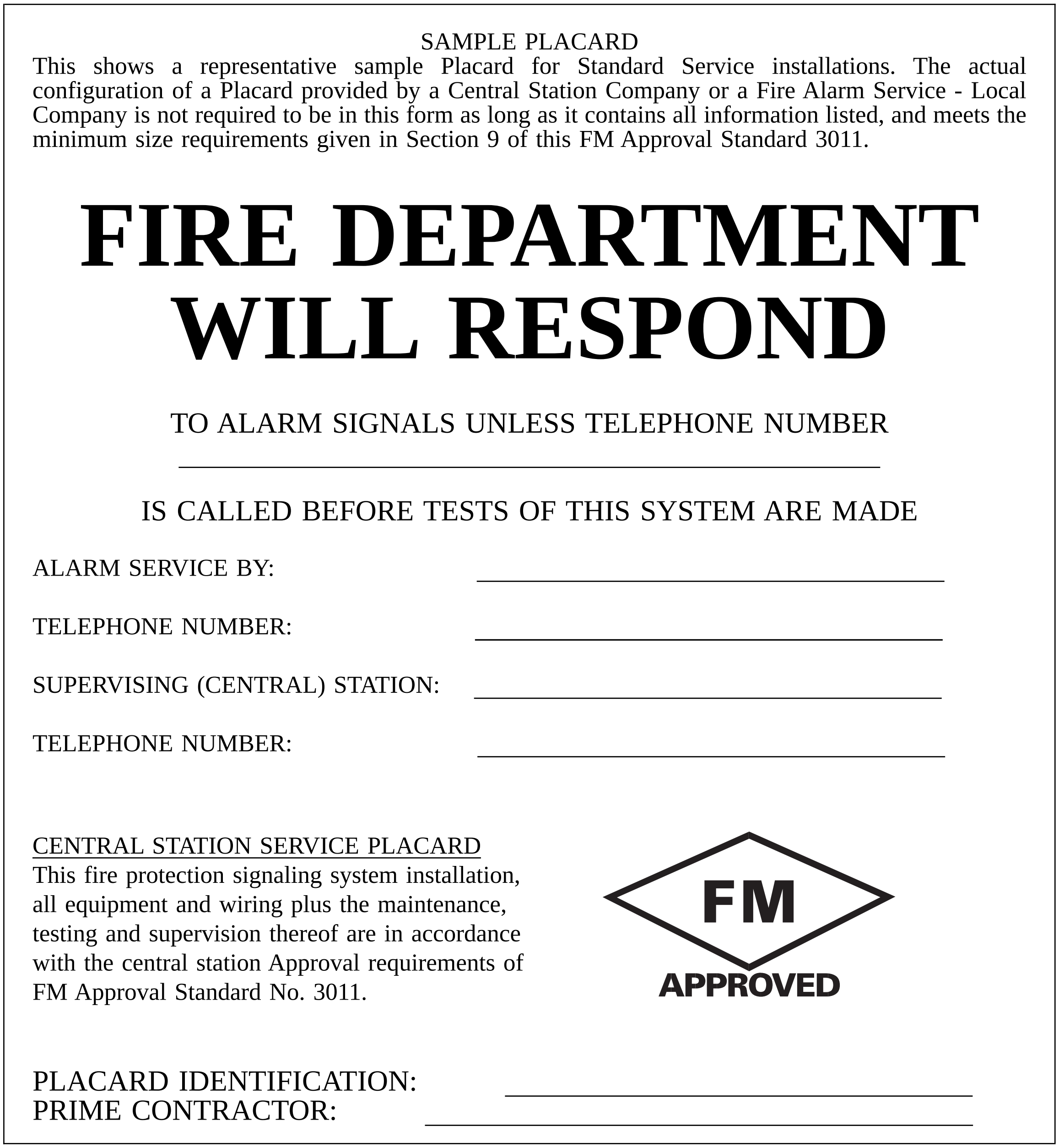
Class IV alarm service means local sprinkler waterflow alarms and other general alarm detection equipment electrically connected with a fire alarm control provided at a location where a response is unreliable. The signaling equipment such as the transmitter, transponder, or digital communicator is not FM Approved and is connected to a constantly attended but not FM Approved proprietary system, remote location, or central station.

Alarms that cause a siren or other type of horn to sound at a constantly attended fire station are also considered Class IV. Class IV alarms also consist of service provided by a central stations, or proprietary systems.

Central stations that are not FM Approved often provide less than what FM considers “Standard Service.” Examples:

- Using equipment that is not FM Approved at the protected premises.
- Testing equipment at the protected premises less frequently than required.
- Subcontracting the installation, or hiring a contractor who is not FM Approved to maintain the equipment.
- Failing to notify the fire service immediately when alarm signals are received.
- Failing to provide maintenance service on nights, weekends, or holidays.

Class IV alarms also consist of “Nonstandard Service” provided by an FM Approved central station or remote supervising station. Unless the installation bears the FM Approval mark and a sign like the one shown in Fig. 2, it is considered by FM to be nonstandard, Class IV.



SAMPLE PLACARD

This shows a representative sample Placard for Standard Service installations. The actual configuration of a Placard provided by a Central Station Company or a Fire Alarm Service - Local Company is not required to be in this form as long as it contains all information listed, and meets the minimum size requirements given in Section 9 of this FM Approval Standard 3011.

FIRE DEPARTMENT WILL RESPOND

TO ALARM SIGNALS UNLESS TELEPHONE NUMBER

____

IS CALLED BEFORE TESTS OF THIS SYSTEM ARE MADE

ALARM SERVICE BY: ______________________

TELEPHONE NUMBER: ______________________

SUPERVISING (CENTRAL) STATION: ______________________

TELEPHONE NUMBER: ______________________

CENTRAL STATION SERVICE PLACARD

This fire protection signaling system installation, all equipment and wiring plus the maintenance, testing and supervision thereof are in accordance with the central station Approval requirements of FM Approval Standard No. 3011.

FM
APPROVED

PLACARD IDENTIFICATION: ______________________
PRIME CONTRACTOR: ______________________

Fig. 2. FM placard for central station service

C.5 Class V: Standard Service, Supervised Waterflow to a Constantly Attended Location, Reliable Response

For Class V alarm service, supervised circuits electrically transmit sprinkler waterflow alarms and other general alarms via FM Approved signal transmitting equipment to an FM Approved central station, a constantly attended proprietary supervising station, or a constantly attended public fire service. Class V service requires mandatory waterflow alarm monitoring. It does not require other system functions, such as sprinkler control valve supervision, water-level monitoring for tanks, fire pump supervision, etc.

All Standard Service Class V alarms, such as sprinkler waterflow, pull station, smoke detection, or heat detection, are transmitted automatically to the remote station, proprietary station, or central station's receivers where trained personnel are in attendance at all times. Central Station Standard Service Class V installation and equipment bear the FM Approval mark and a sign like the one shown in Fig. 2. Class V alarms also consist of a direct connection to constantly attended fire services. In addition, these systems promptly detect circuit faults such as ground fault and open circuit. Class V alarms can also be transmitted to a constantly attended fire service by means of a remote supervising station system or an auxiliary system. The *Approval Guide* listings identify each of these categories and the required equipment to look for.

C.6 Class VIA: Standard Service, Supervised Fire Alarms, Off-Normal Conditions, and Other General Alarms to a Constantly Attended Location, Reliable Response

Standard Central Station or Proprietary System alarm service can be provided by an FM Approved central station or by an FM Approved proprietary system that monitors sprinkler waterflow alarms, supervisory alarms for sprinkler control valves, and other system functions. Each type of signal is coded or uniquely identified so that it may be interpreted properly. This method may be termed Class VIA. Class VIA Service includes monitoring the following:

- Sprinkler waterflow alarms
- Sprinkler control valves larger than 1 in. (38 mm) or valves that control more than five sprinklers.
- Pressure for dry-pipe sprinkler systems and fire protection pressure tanks.
- Fire pumps as recommended in the appropriate FM data sheets.
- Water level within allowable limits in fire protection water storage tanks.
- Heat detectors and/or smoke detectors where applicable.
- Burglar alarms where analysis of the occupancy justifies them.

Unless all applicable functions are monitored, the service cannot be classified as Class VI.

The above systems have maximum reliability and will respond promptly in case of fire, sprinkler leakage, or other trouble.

C.7 Class VIB: Supervised Waterflow to a Constantly Attended Public Fire Service, Standard Service, Supervised Fire Alarms, Off-Normal Conditions, and Other General Alarms to a Constantly Attended Location, Reliable Response

A level of supervisory performance higher than Class V, but not fully meeting Class VIA, can be accomplished by connecting the waterflow alarm to the constantly attended public fire communications center and the remaining functions to an FM Approved central station or a proprietary supervising station using FM Approved proprietary signaling system equipment.

APPENDIX D BIBLIOGRAPHY

American Society for Industrial Security (ASIS). *Guideline for Facilities Physical Security Measures.* ASIA GDL FPSM. 2009.

International Standards Organization (ISO)/ International Electrotechnical Commission (IEC). *Information technology - Security techniques - Information security management systems - Requirements.* ISO/IEC 27001. Second edition, 2013.

National Fire Protection Association (NFPA). *Guide for Premises Security.* NFPA 730, 2014.

National Fire Protection Association (NFPA). *Standard for Security Services in Fire Protection.* NFPA 601.

National Fire Protection Association (NFPA). *Standard for the Installation of Electronic Premises Security Systems.* NFPA 731.

National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013.

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing Security Controls in Federal Information Systems,* December 2014.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers,* October 2006.

Telecommunications Industry Association (TIA). *Telecommunications Infrastructure Standard for Data Centers.* TIA-942-A. March 2014.