
Security Program and Policies

Principles and Practices

by Sari Stern Greene



Chapter 7: Physical & Environmental Security

Objectives

- ❑ Define the concept of physical security and how it relates to information security
- ❑ Evaluate the security requirements of facilities, offices, and equipment
- ❑ Understand the environmental risks posed to physical structures, areas within those structures, and equipment
- ❑ Enumerate the vulnerabilities related to reusing and disposing of equipment
- ❑ Recognize the risk posed by the loss or theft of mobile devices and media
- ❑ Develop policies designed to ensure the physical environmental security of information, information systems, and information processing and storage facilities

Understanding the Secure Facility Layered Defense Model

- If an intruder bypasses one layer of controls, the next layer should provide additional defense and detection capabilities
- Both physical and psychological
 - The appearance of security is deterrent

How to Secure the Site

- All implemented controls to physically protect information are dictated first by a thorough analysis of the company's risks and vulnerabilities, along with the value of the information that requires protection
- From what are we protecting information assets?
 - Theft
 - Malicious destruction
 - Accidental damage
 - Damage that results from natural disasters

How to Secure the Site cont.

- The design of a secure site starts with the location
- Location-based threats
 - Political stability
 - Susceptibility to terrorism
 - Crime rate in the area
 - Roadways and flight paths
 - Utility stability
 - Vulnerability to natural disasters
- Critical information processing facilities should be inconspicuous and unremarkable

How to Secure the Site Cont.

- The physical perimeter can be protected using:
 - Berms
 - Fences
 - Gates
 - Bollards
 - Man traps
 - Illuminated entrances, exits, pathways, and parking areas
 - Manned reception desk
 - Cameras, closed-circuit TV, alarms, motion sensors
 - Security guards

How Is Physical Access Controlled?

- Physical entry controls:
 - Access control rules should be designed for:
 - Employees
 - Third-party contractors/partners/vendors
 - Visitors
 - Visitors should be required to wear identification that can be evaluated from a distance, such as a badge
 - Identification should start as soon as a person attempts to gain entry

How Is Physical Access Controlled? Cont.

- Physical entry controls:
 - Authorized users should be authorized prior to gaining access to protected area
 - Visitors should be identified, labeled, and authorized prior to gaining access to protected area
 - An audit trail should be created

Securing Offices, Rooms, and Facilities

- ❑ The outer physical perimeter is not the only focus of the physical security policy
- ❑ Workspaces should be classified based on the level of protection required
- ❑ Some internal rooms and offices must be protected differently
- ❑ Parts of individual rooms may also require different levels of protection, such as cabinets and closets

Working in Secure Areas

- ❑ Goal: Define behavioral and physical controls for the most sensitive workspaces within information processing facilities
- ❑ Policy controls are in addition to – and not in place of – existing physical controls, unless they supersede them
- ❑ Policy should include devices not allowed on premises, such as cameras, smartphones, tablets, and USB drives
- ❑ Sensitive documents should be secured from viewing by unauthorized personnel while not in use
- ❑ Copiers, scanners, and fax machines should be located in nonpublic areas and require use codes

Protecting Equipment

- Both company and employee-owned equipment should be protected
- Hardware assets must be protected from:
 - Theft
 - Power spikes
 - Power loss
- One way to reduce power consumption is to purchase Energy Star certified devices

Protecting Equipment Cont.

- Potential power problems include:
 - Brownout: Period of low voltage
 - Power surge: Increase in voltage
 - Blackout: Interruption or loss of power
- Power equipment that can be used:
 - Uninterruptible Power Supply
 - Back-up power supplies
 - Power conditioners
 - Voltage regulators
 - Isolation transformers
 - Line filters
 - Surge protection equipment

How Dangerous Is Fire?

- Three elements to fire protection
 - Fire prevention controls
 - Active
 - Passive
 - Fire detection
 - Fire containment and suppression
 - Involves responding to the fire
 - Specific to fire classification
 - Class A
 - Class B
 - Class C
 - Class D

What About Disposal?

- Formatting a hard drive or deleting files does not mean that the data located on that drive cannot be retrieved
- All computers that are discarded must be sanitized prior to being disposed of
- Policy should be crafted to disallow access to information through improper disposal or reuse of equipment
 - Disk wiping
 - Degaussing
 - Destruction

Summary

- The physical perimeter of the company must be secured.
- Some internal rooms and offices must be identified as needing more security controls than others. These controls must be deployed.
- Environment threats such as power loss must be taken into account and the proper hardware must be deployed.
- A clean screen and desk policy is important to protect the confidentiality of company-owned data.