

Physical Security

COBIT

Responsibility for Logical and Physical Security

Management should formally assign the responsibility for assuring both the logical and physical security of the organization's information assets to an information security manager, reporting to the organization's senior management. At a minimum, security management responsibility should be established at the organization-wide level to deal with overall security issues in an organization. If needed, additional security management responsibilities should be assigned at a system Data and System Ownership Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

Manage Facilities

Physical Security

Appropriate physical security and access control measures should be established for IT facilities, including off-site use of information devices in conformance with the general security policy. Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to individuals who have been authorized to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism.

Low Profile of the IT Site

IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited.

Visitor Escort

Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.

Protection Against Environmental Factors

IT management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat and humidity). Specialized equipment and devices to monitor and control the environment should be installed.

Uninterruptible Power Supply

Management should assess regularly the need for uninterruptible power supply batteries and generators for critical IT applications to secure against power failures and fluctuations. When justified, the most appropriate equipment should be installed.

Manage Operations

Safeguard Special Forms and Output Devices

Management should establish appropriate physical safeguards over special forms, such as negotiable instruments, and over sensitive output devices, such as signature cartridges, taking into consideration proper accounting of IT resources, forms or items requiring additional protection and inventory management.

HIPAA

Inventory

The formal, documented identification of hardware and software assets

Physical safeguards to guard data integrity, confidentiality, and availability Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. It covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. Physical safeguards must include all of the following requirements and implementation features:

Assigned security responsibility

Practices established by management to manage and supervise the execution and use of security measures to protect data and to manage and supervise the conduct of personnel in relation to the protection of data

Media controls

Formal, documented policies and procedures that govern the receipt and removal of hardware/software (such as diskettes and tapes) into and out of a facility that include all of the following implementation features:

- Access control
- Accountability
The property that ensures that the actions of an entity can be traced uniquely to that entity
- Data backup
A retrievable, exact copy of information
- Data storage
The retention of health care information pertaining to an individual in an electronic format
- Disposal
Final disposition of electronic data, and/or the hardware on which electronic data is stored

Physical access controls (limited access)

Formal, documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed that include all of the following implementation features:

Equipment control (into and out of site)

Documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media

A facility security plan

A plan to safeguard the premises and building (exterior and interior) from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft

Procedures for verifying access authorizations before granting physical access

Formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges

Maintenance records

Documentation of repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors, and locks

Secure workstation location

Physical safeguards to eliminate or minimize the possibility of unauthorized access to information; for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area