
TITLE: **INFORMATION SECURITY: FACILITY ACCESS CONTROL AND SECURITY**

POLICY:

All facilities in which information systems are located are physically protected commensurate with identified threats and risks.

PURPOSE:

Physically protect information assets.

APPLICABILITY:

Hospital staff, employees, owners, custodians, and users of information systems

PROCEDURE:

1. **Facility Access Control**. Physical access to information systems is restricted to authorized workforce members.

    A. The perimeter of facilities that house information systems are physically sound, the external walls are properly constructed and the external doors have appropriate protections against unauthorized access.

    B. Doors and windows of all facilities are locked when unattended. External protections, such as window guards or bars are installed on all windows at ground level and on any other windows as reasonably necessary to prevent unauthorized entry.

    C. Delivery and loading areas have controls to prevent delivery staff from unauthorized access to Information Technology facilities.

    D. The following risk categories are assigned to the facilities:

        a. *Highly-Sensitive* – Areas where highly sensitive information (including Protected Health Information (PHI) is created, received, transmitted or maintained. Only a small, select group of workforce members need access to complete their job duties (e.g., data center, network closet, etc.).

b. *Sensitive* – Areas where sensitive information is created, received, transmitted or maintained. Only a moderately sized group of workforce members need access to complete their job duties (e.g., radiology reading room, medical records department, etc.).

c. *Monitoring-Required* – Areas where large amounts of information are created, received, transmitted or maintained. Large-sized groups of workforce need access to complete their job duties (e.g., inpatient unit, outpatient clinic, public areas such as waiting room, etc.).

E. Owners determine which workforce members are granted physical access rights to *Highly-Sensitive* areas. Physical access rights are periodically reviewed and revised. Consult Information Security Office for appropriate documentation in *Application security documents list: Physical security, media security, media disposal***.** Information Services Department provides "Data Centers" as physical locations that are *Highly-Sensitive*.

F. Departments managing the physical space and institutional functions associated with *Sensitive* and *Monitoring-Required* areas determine which workforce members are granted physical access rights to the area.

G. Workforce members are required to wear visible identification badges. Workforce members are required to report unescorted strangers or anyone not wearing visible identification to the Security Department.

H. All visitors are required to show proper identification and to sign in prior to gaining physical access to areas where information systems are located.

I. The Security department conducts a periodic review of physical access controls used at its facilities to protect information systems.

2. **Facility Security Plan**. The ***Security Management Plan*** implemented by the Security Department details how it protects physical assets in its facilities from unauthorized access, tampering or theft. The plan includes appropriate physical safeguards for electronic information systems, and addresses the following:

A. Identification of information systems and housing areas, and of processes and controls used to protect same from unauthorized access, tampering or theft
B. Action to be taken if unauthorized access, tampering or theft attempts have been made
C. Identification of workforce members' responsibilities within the facility security plan
D. Notification and reporting procedures

3. **Maintenance Records**. For *Highly-Sensitive* areas, repairs and modifications made to the physical security components such as walls, doors, etc. are documented. The owner and custodian of the area are responsible for maintaining this documentation. The documentation may include:

    A. Date and time of repair or modification
    B. Description of physical component prior to repair or modification
    C. Reasons(s) for repair or modification, including any damage and any related security incident, if applicable
    D. Person(s) performing repair or modification
    E. Outcome of repair or modification

4. **Contingency Operations**. Based on institution's Disaster Recovery and Emergency Mode Operation plan in ***Information security: Disaster contingency and recovery plan policy*** (# I250), in the event of a disaster or emergency, appropriately authorized workforce members can enter facilities to take the necessary actions as documented. Such members are authorized by the owners of the information systems, and are permitted to administer or modify processes and controls that protect the security of information.

RESPONSIBILITY:
Security Office, Information Security Office

REFERENCES:
All information security policies
Health Insurance Portability and Accountability Act of 1996, 45 CFR
164.310(a)(1),
164.310(a)(2)(i), 164.310(a)(2)(ii),
164.310(a)(2)(iii), 164.310(a)(2)(iv)

REVIEW/REVISION DATE:
March 2005
June 2009
June 2011
Reviewed: June 2013; **March 2015**