
Department: UW Medicine Information Technology Services

Policy Number: SEC-04.02 – Physical Security Standard

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

Physical security controls and Secure Areas are used to minimize unauthorized access, damage, and interference to information and information systems. Physical security controls are to be appropriate to the identified risks. This guideline can be used to determine appropriate physical security controls.

Definitions

See SEC-REF *UW Medicine Security Program Glossary of Terms*.

Guideline

The UW Medicine Security guideline for physical security includes the following:

- I. Perimeter & Facility Physical Security
- II. Physical Entry Controls
- III. Internal Physical Security Controls
- IV. Data Protection

I. Perimeter & Facility Physical Security Guideline

A Secure Area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of a Secure Area takes into consideration the possibility of damage from fire, water, explosion, civil unrest, and other forms of natural or man-made disasters. Relevant health and safety regulations and standards are taken into account for any potential security threats presented by neighboring premises, for example; leakage of water from other areas.

The following should be considered:

- Are Secure Areas clearly defined?

- Is the perimeter of the building or site containing information processing facilities physically sound (i.e. there are no gaps in the perimeter or areas where a break-in could easily occur)?
 - Are physical barriers, if necessary, extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding?
 - Are doors and windows locked when unattended and is external protection considered for windows, particularly at ground level?
- Are unoccupied Secure Areas (i.e. storage facilities, walk-up computers or printers) protected or secured at all times.
- Are information-processing facilities managed by UW Medicine physically separated from those managed by third parties?
- Do workforce members know the contingency plans for your area including locations of fire alarms and extinguishers, power shut-off and evacuation routes?
- Are emergency numbers posted at convenient locations in the area?
- Have physical security considerations been coordinated with business continuity and disaster recovery planning?
- Is disaster recovery media stored at a remote location?

II. Physical Entry Controls

Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

The following should be considered:

- Access to sites and buildings should be restricted to only authorized personnel. Wherever possible, are staffed reception areas or other means used to control physical access to the site or building? Are visitors to Secure Areas supervised or cleared and their date and time of entry and departure recorded? Are they only granted access for specific, authorized purposes and are provided with instructions on the security requirements of the area and on emergency procedures?
- Is access to sensitive information, and information processing facilities, controlled and restricted to only authorized persons? Are authentication controls (e.g. swipe card plus PIN) used to authorize and validate all access?
- Is an audit trail of all access securely maintained?
- Are all members of the workforce required to wear some form of visible identification and are they encouraged to challenge unescorted strangers and anyone not wearing visible identification?

- Are access rights to Secure Areas regularly reviewed and updated?

III. Internal Physical Security Controls

Internal controls are applied to specific rooms or physical spaces within a building or facility. The following should be considered:

- Are support functions and equipment (e.g. photocopiers, fax machines) placed appropriately within Secure Areas to avoid use which could compromise physical security? Wherever possible, are computers located away from entrance doors and walkways to reduce opportunities for theft or misuse?
- Is an inventory maintained of all of your computer equipment and media to account for RESTRICTED and CONFIDENTIAL information?
- Are door locks, safe combinations, and keypad pin numbers changed at frequent intervals?
- Is CONFIDENTIAL information such as combinations, usernames, and passwords stored securely or memorized instead of written down?
- Are written repair orders that include a description of the equipment and the identity of the person who requested the repair required before releasing hardware components for repairs? Is the identification of all repair personnel and vendors verified?
- Is there an established system to record all property being removed from the facility or building?

IV. Data Protection

The following should be considered:

- Are computer monitors positioned so the display is not readily visible to passers-by or are monitors obscured by other means such as a privacy screen?
- Do only authorized individuals have access to the work area?
- Is removable media stored securely when not in use?
- Are backup copies of important software and data files made?
- Are all classified equipment and media, such as disks and printouts, properly labeled and protected appropriately based on their classification?

References:

- I. 45 CFR Parts 164; Section 164.310(a)(1) Facility Access Controls
 - II. 45 CFR Parts 164; Section 164.310(a)(2) (iii) Access Control and Validation Procedures
 - III. 45 CFR Parts 164; Section 164.310 (c) Workstation Security
 - IV. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 7, Physical And Environmental Security
-
-

UW Medicine IT Services: _____ Date: _____
James S. Fine, M.D., CIO, ISO
