

---

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-04 – Physical and Environmental Information Security Policy

Effective Date: June 11<sup>th</sup>, 2007

Review Date: April 27<sup>th</sup>, 2007

---

---

## **Purpose**

The purpose of this policy is to ensure that appropriate physical and environmental safeguards are put in place to protect and minimize risks to UW Medicine's<sup>1</sup> information and information systems.

## **Definitions**

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

## **Policy**

UW Medicine entities must implement policies and procedures to safeguard their facility (ies) and the equipment therein from unauthorized physical access, tampering, and theft.

The responsibility for physical and environmental information security resides with UW Medicine departments and System Owners.

Departments and System Owners must limit physical access to electronic information systems and the facilities in which they are housed to those individuals who are properly authorized to be on the premises and use the equipment.

System Owners must conduct and document risk assessments to secure the area, protect the equipment, and secure the system. When System Owners

---

<sup>1</sup> UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; Hall Health Primary Care Center; University of Washington Physicians; UW Medicine Eastside Specialty Center; as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.

conduct their risk assessments, they need to include an assessment of the physical risks to the facility, the area, the equipment, and the system. Where appropriate, the Entity's Public Safety Department provides direction and expertise. See UW Medicine Information Security Standard: *SEC-09.01 –Risk Assessment Guideline* for details in conducting Information Risk Assessments.

## **Standards**

Controlling facility access encompasses:

- Establishing procedures for contingency operations. See *SEC-07 Business Continuity Management Policy*
- Controlling and validating individuals' access to facilities based on their role or function and controlling access to software programs for testing and revision. See *SEC-06 Access Control Policy*
- Documenting maintenance and operations that relate to Information security (for example hardware, walls, doors, and locks). See *SEC-05 – Communications and Operations Management Policy*
- Securing the area by safeguarding the facility and the equipment from unauthorized physical access, tampering, and theft.

## **I Secure Areas Standard**

In order to minimize unauthorized access, damage, and interference to information and information systems, System Owners and UW Medicine departments must define what areas are to be treated as secure areas. Based on a physical risk assessment, the System Owner, in conjunction with the UW Medicine department, and the UW Medicine Entity's Public Safety Department, determines the level of protection required for any secure area under his or her control.

### **A) Individuals Working in Secure Areas**

Additional controls may be required for individuals working in secure areas.

Controls for individuals working in secure areas include:

- Un-staffed secure areas are physically locked and periodically checked.
- No photographic, video, audio or other recording equipment is allowed unless specifically authorized.
- Third party support services personnel are granted access to secure areas only when required, authorized, and supervised.

## II. Equipment Protection Standard

Based upon information and/or information system classification, equipment must be protected to reduce risks from environmental threats and hazards and to reduce the risk of unauthorized access to information.

### A) Equipment Location and Protection

The following controls are considered for systems classified as containing Restricted or Confidential information:

- Equipment is located in a physically secure location to minimize unnecessary access.
- Environmental conditions are monitored for conditions that could adversely affect the operation of computer systems.
- System Owners need to consider potential impact of a disaster happening in nearby premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street. See UW Medicine Information Security policy: *SEC-07 Business Continuity Policy*.
- Server Systems must comply with the additional requirements as specified within UW Medicine Information Security standard: *SEC04.01–Secure Server Location Standard*.

### B) Equipment Maintenance

To ensure continued availability and integrity, equipment is properly maintained.

Equipment Maintenance controls includes:

- Maintaining equipment in accordance with the supplier's recommended service intervals and specifications.
- Permitting only authorized maintenance personnel to carry out repairs and service equipment.
- Maintenance by System Operators of records of all suspected or actual faults and all preventive and corrective maintenance. See *SEC-05 – Communications and Operations Management Policy*
- Use of appropriate controls when sending equipment off premises for maintenance. Examples of appropriate controls include proper packaging and sealing of containers, storage in safe and secure places, and clear and complete shipping and tracking instructions.

### C) Removal of Property

Equipment, information or software is not to be taken off-site without authorization.

Where necessary and appropriate:

1. Workforce<sup>2</sup> members must obtain authorization to take equipment off-site;
2. Equipment is logged out;
3. When returned, equipment is logged back in.
4. Workforce members are made aware of potential implications of using mobile computing equipment:
  - Purchase of mobile equipment for staff is implied authorization for being taken off-site.
  - Spot checks may be performed to detect unauthorized removal of property.
  - Security for the equipment used off of UW Medicine premises must be the same as the security used for on-site equipment, taking into account the risks of working outside the organization's premises.
  - Equipment and media taken off the premises are not left unattended in public places. For example: home-working controls are determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, and access controls for computers.
  - Portable computers are carried as hand luggage.

**D) Restricted and Confidential data handling**

Information that is classified as RESTRICTED and CONFIDENTIAL must be handled properly. See UW Medicine Information Security standard: *SEC05.02 Media Handling Standard* for proper handling procedures.

**III. Secure Server System Location Standard**

*Refer to SEC04.01–Secure Server Location Standard.*

**IV. Physical Security Guideline**

*Refer to SEC04.02 - Physical Security Guideline.*

---

***Cross References:***

---

<sup>2</sup> Workforce: Faculty, employees, trainees, volunteers, and other persons who perform work for UW Medicine, and whose work conduct is under UW Medicine's direct control regardless of whether or not the workforce member is paid by UW Medicine.

*HHPCC: HHPCC Administrative Manual - Section 9 – Safety, Security & Emergency Preparedness*

*HMC: HMC APOP 50.03 Environment of Care Management Plan*

*SOM: HSAS&F Security Management Plan (or Facility Security Plan)*

*Sports Medicine Clinic: SMC Privacy and Security Policies Manual “Sports Medicine Security Management Plan”*

*UWMC:*

*UWP:*

*UWPN: Electronic Medical Record  
Information Systems Usage and Equipment  
Photo Identification Badges  
Epic Downtime and Power Outages  
Handling Medical and Non Medical Emergencies*

---

---

**References:**

- I. 45 CFR Parts 164; Section 164.310(a)(1) Facility Access Controls
- II. 45 CFR Parts 164; Section 164.310(a)(2) (ii) Facility Security Plan, (iii) Access Control and Validation Procedures, (iv) Maintenance Records
- III. 45 CFR Parts 164; Section 164.310 (c) Workstation Security, (d) (1) Device and Media Controls
- 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

---

---