
Department: UW Medicine Information Technology Services

Policy Number: SEC-05.04 Minimum Workstation and Server Information Security Standard

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

The purpose of this standard is to document UW Medicine minimum requirements for all workstations and servers on the UW Medicine networks, and document proper security procedures.

Standard

It is UW Medicine¹ policy that System Owners ensure all computers meet the following minimum requirements:

1. Use only operating system versions that have current security update support. Consult with your operating system vendor to determine product lifecycle and security support policies.
2. Do not connect any system directly to the University of Washington network or a networked device until the system has been properly configured and secured. Build computer systems off the network or while behind other network-based firewall protection.
3. Follow appropriate operating system hardening guidelines, <http://security.uwmedicine.org/resources/default.asp>.
4. Use strong passwords for all accounts. (See Information Security Policy; *SEC 06 – Identity and Access Management Policy*)
 - a. Ensure that no built-in accounts have blank, weak, or well-known passwords.
 - b. Ensure that all passwords provided with vendor products are changed from their defaults.
 - c. Protect administrative accounts with stronger passwords and/or more frequent rotation.

¹ For the purposes of HIPAA, 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.

5. Apply all major operating system and application service packs or updates in a timely manner. Ensure security patches are installed in a timely manner between major service packs and updates.
6. Block unnecessary or potentially malicious network traffic through use of a firewall or other forms of network traffic filtering.
7. Reduce the risk of infection and spread of malicious software through use of anti-virus, anti-spyware, and system integrity enforcement software as appropriate to your operating system. Ensure updates are installed in a timely manner.
8. Enable the logging of important security related events.
9. Acquire an appropriate IP address.
 - a. Obtain a dynamic or static IP address through an IT Services Help Desk or UW Technology or other UW Medicine approved DHCP server, **or**
 - b. Use a private IP address that is logically separated from the University of Washington IP network.
10. Ensure that appropriate data classification has been documented (See Information Security Policy; *SEC-02 – Information and Information System Classification*)

Additionally, System Owners of UW Medicine Servers must meet the following requirements:

1. Review system and security logs regularly. Investigate, report, and correct irregularities as appropriate.
2. Create and maintain a server backup and restoration plan. (See Information Security Policy; *SEC-05 – Communications and Operations Management Policy*)
3. Implement appropriate environmental and physical security controls. (See Information Security Policy; *SEC-04 – Physical and Environmental Information Security Policy*)
4. System Owners must certify that servers are in compliance with all UW Medicine Information Security Policies.

UW Medicine IT Services: _____ Date: _____

James S. Fine, M.D., CIO, ISO
