UNIVERSITY OF WASHINGTON SCHOOL OF MEDICINE

DEPARTMENT OF RADIOLOGY
POLICIES AND PROCEDURES

Policy Title: IT System Administration	**Approvals:**
Reference Number: Fiscal 2007-08	Norman J. Beauchamp, Jr, MD — Date: 12/14/7
Effective Date	Responsible Administrator/Manager — Date: 12/13/07

Scope

This policy applies to the following:

* Any computer hardware or software purchased through Department of Radiology budgets including state or federal funds
* Any device that communicates on a University of Washington network whether on campus or a remote site which is under the supervision of the Department of Radiology
* Any computing related device in any University of Washington facility that is under the supervision of the Department of Radiology

Overview

The Department of Radiology Information Technology team and the Administrative Services team are responsible for adhering to and enforcing University of Washington policies regarding computer and network infrastructure in the Department of Radiology. This policy outlines processes to be implemented by the department's IT System Administrators to ensure that systems are adequately maintained.

These guidelines are a supplement to the basic UW policy on ethics in computer use and the University's software copyright policy.

The computing and networking infrastructure of the University of Washington underlies many crucial activities for the entire University community, including hospitals and clinics. The University's primary responsibility is to protect and sustain the operation of those facilities. As such, the University may take whatever steps it feels appropriate to remedy or prevent activities that, in the University's judgment, endanger the orderly operation of University's networks or systems, and/or which threaten the University's network connections to the Internet and/or other institutions or networks.

Definitions

System: A network, computer, software package, or other entity for which there can be security concerns.
System Administrators: Individuals who support the operations and integrity of computing systems and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. In addition, managing the computer network is often their responsibility in an inter-networked computing environment.

Processes

1. Operating systems and applications must be maintained with the timely application of all related vendor-issued patches necessary to prevent the systems from being compromised and/or causing disruptions of network services and/or other systems.

2. Externally accessible systems must install antivirus software and maintain procedures for regular signature updates.

3. Shared systems are required to have a technical access control mechanism that allows authorization and allocation of system and data resources to individual users.

4. Procedures must be maintained for regular backup of all data and system files necessary for discovery and recovery purposes. All backup media should be stored properly in a location authorized by the data owner with protections that allow access to the data by authorized personnel only. The ability to recover data from backups should be tested regularly.

5. Shared systems are required to have the capability to log basic information about user access activity, system changes, and events for the possible creation of historical logs and access violation reports. Logs must be monitored for intrusions or attempts at unauthorized access.

6. Systems must maintain a functioning and accurate system clock, since it is a critical element for the computer forensics and system logs that are essential for successful investigations.

7. Encryption capabilities (the ability to turn readable text into unreadable cipher text) must be used for systems that send or receive personally identifiable information that is transmitted over open networks like the Internet or UW-owned networks.

8. Critical servers must be housed in protected areas such as server sanctuaries (locations where suitable physical and logical security measures can be implemented). (See UW Guidelines for Implementing Systems and Data Security Practices.)

Reference the following UW Policies:
Web site for UW Information Systems Security:
http://www.washington.edu/admin/rules/APS/02.01TOC.html

Policy:

Responsibilities:
Chris Laubenthal
John Powell
David Curulla
Cris Ewing

Notes:

1. **Dates of official enactment and amendments:**
2. **Cross References:**