Academic Health Center – Information Systems

Subject: AHC Workstation Standards
Policy No.: 9002
Applicable to: AHC Workstations on the University Network
Pages: 3
Author: Ed Deegan, Director – AHC-IS
Date: 8/12/13
Replaces version dated: FY13

POLICY: Academic Health Center Workstation Standards

Introduction
The purpose of this standard is to define acceptable levels of support and best practices for management of computer workstations and laptops within the Academic Health Center (AHC). These standards are intended to match or, in some cases, exceed standards established by the University of Minnesota, Office of Information Technology (OIT) for workstation management.

The AHC requires a high level of technical support and security for workstations because private and non-public data exists across all levels of the organization.

Continuity of support for private data: Units that have a substantial portion of their activity involving access or storage of private or non-public electronic data should assume that the entire unit accesses or stores private data and that all electronic devices need to be secured. In such an environment, it is likely that access to (or physical transfer of) such data will occur on a regular basis.

These standards are needed to ensure data is available on a reliable basis and that data integrity and security are not compromised by malicious activity. The ever increasing attacks from computer "hackers" require a high level of expertise and vigilance in protecting AHC workstations and associated data. This standard defines the management and support practices for these AHC resources.

Definitions
This AHC standard references the following definitions:

- Workstation – The term "workstation" refers to any Windows or Macintosh desktop or laptop computer accessing or connected to the University network, either through an EtherJack or wireless connection.

Annual Review and Compliance
All AHC workstations will be subject to review for compliance with this standard. Included are review of required documentation, staffing levels, and practices.

Workstation Identification
All University owned workstations connected to the University network must have a physical identifier attached indicating which person(s) or organization is responsible for technical support. This identifier can be a label, sticker, etc. attached to the monitor, screen, or CPU cabinet. Information on that identifier must include:

- Organization name who is providing technical support
- Contact phone number or e-mail

Workstation Tracking
An inventory of all supported workstations and laptops must be maintained by the supporting technical unit. The inventory must be maintained on a daily basis and be available for review by appropriate University or AHC technical staff. The inventory must capture basic information about the hardware including, but not limited to, the following:

- Computer model and type
- Location
- Purchased or installed date
- Basic information about the hardware
Operational Maintenance & Security Standards
Operational security involves the ability to secure both hardware and data from unauthorized access. All workstations and data must conform to the following aspects for security:

Windows Machines

- When properly configured, Windows XP and System 7 operating systems are considered "secure". Older operating systems must be upgraded.
- Anti-virus software must be installed and operational on all workstations. Updates to the anti-virus software must be performed on a daily basis.
- Operating system and application patch management must occur in one of the following ways:
  - Patch management software must be installed on each workstation with the ability to “push” patches to each workstation from a centrally managed server, and/or
  - Windows updates must be configured to download AND install updates automatically and this cannot be disabled by the user. If using this method, the computer should be rebooted within 24 hours of patch installation.
- A password protected screen saver must be used to prevent unintentional keyboard activity.
- Administrative accounts must be restricted to a limited set of trained / qualified I.T. staff responsible for maintaining and managing the workstations. A case by case exception for user “elevated privileges” may also be granted to the user by the I.T. unit. These exceptions must be documented by the I.T. unit.
- Windows Firewall must be active.
- Software should only be installed by qualified I.T. professionals responsible for supporting the workstations. A case by case exception for user software installation may also be granted by the I.T. unit.
- A "security template" must be applied to each workstation that complies with University OITs' Enhanced Security for Computers and Other Electronic Devices – see [http://www.policy.umn.edu/Policies/it/Use/SECUREDATA_PROC02.html](http://www.policy.umn.edu/Policies/it/Use/SECUREDATA_PROC02.html)
- Insecure or unnecessary services, (e.q. Windows File & Print sharing, Net Bios, etc.) must be uninstalled or disabled.
- Users must be required to enter a username/password each time (s)he logs onto the machine (i.e., auto-login should be disabled).
- Windows workstations should be supported though an “OIT Approved” Active Directory management environment. Exceptions may be allowed for certain workstations that do not function correctly in an AD domain (e.g. lab devices, etc.). Processes and policies should be defined to evaluate and manage any exceptions.

Macintosh Machines

- When properly configured, OSX (Ten) is considered a “secure” operating system; older versions must be upgraded.
- Anti-virus software must be installed and operational on all workstations and must be configured to update virus definitions at least once a day during normal business hours.
- A password protected screen saver must be enabled to prevent unintentional keyboard activity.
- Automatic updates must be configured in the System Preferences control panel to download and install "important updates" on a daily basis.
- Users must not use the default administrator account for daily activities such as e-mail or word processing. Any "shared" accounts should only be established by I.S. staff.
- Automated login (i.e. users must enter username/password), display of user names, and password hints must be disabled.
- Internet Connection Sharing must be disabled.
- “Bluetooth” must be disabled unless required. If Bluetooth is required, users must ensure that discoverability is unchecked to prevent devices from finding your computer.
- Firewalls must be enabled with the exception that Network Time Protocol and logging are allowed.
- Security settings on all Macintosh devices should conform to the OIT standards.
Laptop Computers
- Private data on AHC laptops must be encrypted to the levels established by AHC-IS.
- USB storage devices and external hard drives should utilize 256 bit hardware based encryption.
- All AHC workforce members and volunteers must take steps to appropriately provide for the physical security of laptops and other mobile devices. Use of cable locks is the most common solution.

Staffing levels / Technical Management Skills
Workstations and associated software applications must be supported and managed by I.T. staff with appropriate technical expertise and experience.
  - A typical I.T. staffing position would equate to a full-time Information Technical Professional position per University job classifications. (Or a portion of a shared FTE University staff person).
  - Non-university technical staff \ consultants must meet similar requirements before being placed under contract at the AHC.
    - Documentation covering work expectations and responsibilities must be developed prior to contract personnel beginning work at the AHC.
    - Typical items that must be documented for contract workers \ consultants include:
      - Hours of support or availability.
      - Proof of liability insurance (required on University contracts).
      - Written acknowledgement by the contractor of their security responsibilities and precautions.
      - General assessment of their prior pertinent technical experience and education.
  - Depending upon defined work or office hours of operation, there must always be an I.T. support person available for support. This will require availability of two trained I.T. staff for coverage of vacations and absences.
  - There must be some form of “Help Line” (telephone, e-mail, etc.) available for the supported users to request assistance from the designated technical support person(s) or unit.
  - All technical support activity or services performed on workstations should be documented or logged in order to maintain a “change control” history for each device.