

---

<b>Subject:</b> AHC Server Standards	<b>Policy No.</b>	9001
<b>Applicable to:</b> All AHC Servers on University Network	<b>Pages:</b>	4
<b>Author:</b> Ed Deegan, Director – AHC-IS	<b>Date:</b>	7/18/05
	<b>Replaces version Dated:</b> NA	

---

**POLICY: Academic Health Center Server Standards**

***Introduction***

The purpose of this standard is to define acceptable levels of support and best practices for management and support of computer servers 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 server management.

The AHC requires a high level of technical support and security for servers because non-public data exists across all levels of the organization. This approach is consistent with University policy Academic/Administrative policy 2.8.1 - Acceptable Use of Information Technology Resources - Appendix M: Information Technology Support Guidelines states,

- o " **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 the 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 servers and associated data. This standard defines the management and support practices for these AHC resources.

***Definitions***

This AHC standard references OIT's Guideline – Critical Server Identification document for the following definitions:

- o Server - a multi-user computer, which provides some service for other computers connected to it via a network. The most common examples are departmental/collegiate file servers, web servers, mail servers, and database servers.
- o "Critical" Server – a server important to accomplishing the University/collegiate unit/business unit mission or which stores legally protected or other important non-public data.

***Documentation Requirements***

Complete and current documentation is required to support and validate the overall management practices of the I.S. staff. Following are examples of documentation that should be on file:

- o Listing of all personnel with physical access to servers.
- o Disaster Recovery Document – see below for details.
- o Data protection \ preservation processes – description of backup processes.
- o Server account management policies.

### **Annual Review and Compliance**

All AHC server sites \ data centers would be subject to review for compliance to this standard. Included would be review of documentation, tour of server facility, and discussion of current staffing levels and practices.

### **Physical Security Standards**

All servers must be located in a separate facility designed or dedicated for that purpose. The facility should have the following attributes:

- Uninterruptible Power Supply (UPS) supporting all servers and essential peripheral equipment (monitors, KVM switches, etc.).
- Climate controlled environment separate from the building HVAC, (dedicated air conditioning with in-room temperature controls).
- Secured access to the facility with documentation listing all individuals who currently have access.
- The facility should have the ability to quickly change “access codes” (not key locks) if personnel changes warrant.
- The facility should have basic fire suppression services, (i.e. sprinklers, extinguishers, etc).

### **Operational Security Standards**

Operational security involves the ability to secure both hardware and data from unauthorized access. All servers and data must conform to the following aspects for security:

- Firewall or communication filtering must be used to limit network access to hardware and software:
  - All servers and data must reside behind some type of “Firewall – communication filtering” technology to help protect it from outside intrusion originating from the network.
  - Firewalls can consist of hardware / software solutions, network infrastructure, or selected communication restrictions such as IP or Port filtering.
  - The I.S. staff should have the ability to produce “audit” or “usage” reports documenting user access and network activity to the critical servers housing non-public data staying consistent with AHC procedures and University policy.
  - Written documentation must be available describing firewall or filtering rules currently used in the server facility.
- Anti-virus software must be installed and operational on all servers (per University policy). Updates to the anti-virus software must be performed on a daily basis to ensure up-to-date protection.
- Servers should utilize “keyboard locking” software or password protected screen savers to prevent unintentional keyboard activity.
- All critical servers must be registered with OIT Security for scanning and monitoring purposes. Information provided to OIT Security should include:
  - Server identification / IP address.
  - Purpose of server.
  - Location of the server.
  - Data Owner(s) and listing of categories of non-public data.
  - Names & emergency contact information of support personnel.

- Restriction to Root \ Administrative Accounts
  - Administrative functionality needs to be restricted to a limited set of trained \ qualified I.S. staff responsible for maintaining and managing the server. Documentation should exist listing I.S. staff and their administrative responsibilities for each server \ application \ database.
  - Administrator accounts should use a strong “password phrase” making it less likely the password can be compromised by password cracking software.
  - Administrator accounts should only be used for tasks relating to server administration duties, not normal user-related tasks.
  - Each individual administering a server should have a unique administrative account and password to better distinguish activities between various administrators.
- User Accounts on Servers
  - All individuals accessing servers, applications, or shared data should have a unique User Account or “Login ID”.
  - “Shared or Guest” IDs are not permitted on any server housing non-public data.
  - User account passwords are required on all user accounts.
    - Passwords should be changed at a minimum every 180 days.
    - Seven character limit minimum for passwords.
    - Upper / lower case and numeric combinations recommended.
    - Passwords should not be configured or checked as to be “Remembered” on applications.
  - User account management
    - There should be a documented process for creation \ modification of user account rights. The process should include some method of “supervisor approval” to initiate the creation \ modification of a user account.
    - I.S. staff should have the ability to verify or report on access capability of any user to a particular server or dataset.
    - I.S. staff must have the ability to identify inactive accounts and purge user accounts (and associated data) from the server after a specified time of inactivity (inactivity timeframe can be established by the I.S. staff).
- All Operating Systems, software applications, etc. must be properly configured and patched to vendor specifications \ University OIT \ AHC security guidelines and standards.
  - I.S. staff must regularly monitor University Security notifications regarding the latest security threats, patches, and University network activities.
- Documentation or logs should be maintained indicating current versions of OS and software running on servers including when last updates \ patches were performed and which I.S. staff did the work.

### **Data Protection and Preservation**

I.S. staff must have safeguards in place to ensure data preservation for all servers:

- Backup processes should be in place to support all data and information stored on the servers. Industry accepted technology, utilizing tape, SANS, offsite storage, etc. must be in place and supported to ensure data protection.
- Off-site storage of backup media or data is required and must adhere to the same level of security as defined above for servers \ data. (Daily offsite storage recommended).

- 
- The retrieval process for both media \ data must be documented and available for review.
  - I.S. staff should publish the retention schedules of archived data and associated backup media for their user community.
  - Any storage media, (disks, tape, semiconductor, etc.) must have all data deleted prior to disposal. Deletion should be performed using a process specifically designed for secure purging of data from storage media.
  - Written documentation should be on file describing all processes and procedures supporting the above activities.

### **Disaster Recovery – Operational Continuity**

I.S. staff must develop and maintain a Disaster Recovery \ Operational Continuity plan. Such a plan would contain the following information:

- A listing of all servers supported, including the following details:
  - Server name.
  - Hardware configuration (platform, memory, speed, etc.).
  - Purpose (mail, file sharing, web host, database, etc.).
  - Any IP numbers associated with the server.
  - Physical location of the server (room number).
  - Any pertinent applications or services running on the server.
  - A notation if the server contains non-private data and the nature of that data.
  - A notation of the critical nature of the server (see OIT Critical Server Guideline).
- A step by step “Start-up process” for each server. The process should consist of each step needed to bring up the server and all services from a cold-boot condition.
- A listing of vendor maintenance contracts and the process to request replacement hardware and software products in the case of failure. Associated contract information would include:
  - Contract numbers of the vendor agreements.
  - Hardware serial numbers or software license numbers.
  - Vendor phone numbers – where to call when help is needed.
  - Expiration dates of the support agreement and other pertinent details.
- Documentation on the data backup process:
  - Should include the retention schedule and tape locations.
  - Should document the process to recover data from backup.
- Emergency call list of those individuals who would respond to a server failure.
- A priority list identifying which server or service would be restored first in the event of a multi-server failure.
- I.S. staff should conduct an annual review of the disaster plan.

### **Staffing levels / Technical Management Skills**

Servers and associated software applications must be supported and managed by I.S. staff with appropriate technical expertise and experience.

- A typical I.S. 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 \ ASPs should meet similar requirements before being placed under contract at the AHC.
    - Documentation covering work expectations and responsibilities should be developed prior to contract personnel beginning work at the AHC.
    - Typical items that should 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 hours of operation for the servers, there should always be an I.S. support person available for support. This will require availability of two trained I.S. staff for coverage of vacations and absences.