Section:	Information Security	Effective:	December 2005
Standard:	Server Security Standard	Revised:	
Policy Ref:	5.8.14 Administration of Security on Server Computers	Responsibility:	Chief Information Security Officer

SERVER SECURITY STANDARD

Security Standards are <u>mandatory</u> security rules applicable to the defined scope with respect to the subject.

Overview

Improperly configured systems, including both servers and workstations, can be compromised and the data destroyed or stolen, or used to store illegal data, relay spam e-mail, or attack other systems.

Scope

All authorized users including but not limited to faculty, staff, students, contractors or guests who have or are responsible for administration of any computer system that functions as a server on the UTHSCSA network.

Purpose

The purpose of this document is to establish a standard for securing and documenting server systems at UTHSCSA.

Instructions

This section lists items that are required and/or recommended for all servers at UTHSCSA. Items marked as *required* are mandatory and may be used in system administrator qualification and as auditable items in an IT security audit. This standard is established as part of the requirement of HOP policy 5.8.14 "Administration of Security on Decentralized Server Computers", but will also be used as security standards for centralized servers where applicable.

QUALIFIED SERVER ADMINISTRATOR: *(Required)*

- **A**ll decentralized servers must be managed by an administrator who is qualified by the UTHSCSA Information Security Office for security administration on that specific type of server.
- The designated administrator need not be in a full time technical or computer-related job function, but must be capable of the required technical knowledge and skills and must be given sufficient work time to manage and maintain the server.
- In order to become a qualified system administrator, an individual must:

1. Agree to and **sign a standard ethics agreement** regarding security administration.
2. **Enter applicable information for servers into the Server Inventory Database**, with one record for each of the servers to be administered by the individual.
3. **Have the inventory records reviewed and approved** by an Information Security Officer in the process of a security qualification interview.
4. **Complete required security awareness training** – currently this requirement consists of viewing the TSR Basic Security Awareness Training

modules 1 & 2.

SEPARATION OF FUNCTION: ***(Required)***

- Servers should **never** be used as an individual's primary workstation (even the system administrator) since normal user activities such as web surfing, mail reading, etc. can introduce a significant risk of compromise onto the server.
- Servers must be designed in a way that allows services, applications, and data to be grouped or separated according to data classification and function.
- Servers must be protected to the level required to safeguard the highest risk data or applications they contain.
- Servers that are used to house sensitive information such as identifiable patient data or financial or student records should be used for that function only, with physical and logical access to the server limited as much as possible to only those users who legitimately need to access the data.
- Servers housing sensitive information **should not** also be used to serve less sensitive local or public data or to host any high-risk application such as a public web page, ftp server, departmental file server, or decentralized mail server.
- Even servers that host only public data or high-risk applications should have separation of function as much as possible, since each application or service on the server increases complication and administrative burden, and the risk to all other data or applications on the server.
- Web-based database applications must be developed in a two-tiered architecture that places the web front end on a different server than the back-end database.

SERVER HARDENING: ***(Required)***

- All servers must, to the extent possible for the operating system, application, and function, be configured in a way that reduces the risk to the system through the elimination of unneeded services and their vulnerabilities.
- Actual hardening techniques vary according to operating system, but some issues involved in hardening include:

    - Physically securing the server and console operations
    - Elimination of unnecessary services
    - Minimization of unneeded startup scripts or scheduled processes
    - Reduction of available network connectivity
    - Management of file and directory permissions
    - Establishing restrictions on user access
    - Configuring server operations to maintain appropriate separation of function

- Installing utilities or management software to strengthen or simplify administration

- Some hardening issues are covered further in the general server security standards presented in this document. Other hardening issues may be specific to a particular operating system. Guidelines for hardening specific types of operating systems are provided on the Information Security website at http://infosec.uthscsa.edu/hsc_secpol/Guidelines/guidelines.html.

(Where Possible)

- On servers that are considered a critical resource or that house critical functions, consider implementing security features such as load balancing or hardware redundancy for high availability.

PASSWORDS: ***(Required)***

- Password administration for local and decentralized domain user accounts must conform to the established UTHSCSA password standard.

BACKUPS: ***(Required)***

- All servers must have an established, documented, and consistently used backup plan. Specific components of the plan are to include:
  - Backup and media rotation schedule planning must take into account the data classification and criticality, and any regulations or document retention requirements that apply to the data being backed up. Information for required records retention for UTHSCSA can be found at http://www.library.uthscsa.edu/services/records/records.cfm .
  - Backup media must be stored in a secure location at a safe distance from the server.
  - Backup media and the backup plan must be tested regularly to ensure that backups are usable and the plan is sufficient to provide the required data protection.
  - Sufficient backup media for disaster recovery of the operating system, data, and applications must be stored in a secure location (offsite) far enough away from the server to reduce the risk of catastrophic loss and unrecoverable data in the event of a disaster.
  - It is the responsibility of the system administrator in cooperation with the data owner to determine the appropriate frequency and retention of data backups.

Guidelines for establishing a backup plan can be found on the InfoSec website at http://infosec.uthscsa.edu/hsc_secpol/Guidelines/guidelines.html.

REMOTE ACCESS: ***(Required)***

- Internal connections can use any valid protocol but connections to non-public IT resources must be authenticated.
- External connections to any non-public IT resource must use an encrypted protocol such as Virtual Private Networking (VPN), Secure Shell (SSH), Secure FTP (SFTP), secure web services (SSL or HTTPS), etc.
- Servers that require remote access for vendor support or administration should allow for encrypted access through SSH or other server-based facility, or the vendor must be supplied with a guest account and access the server through the vendor VPN client distributed by T&N.

(Where Possible)

- Internal connections should also utilize encrypted protocols to further reduce the risk of interception or other malicious interference in the connection.

SHARED OR REMOTELY MOUNTED RESOURCES: *(Required)*

- Except for public IT resources, all shared or mapped folders, drives, and devices must have connection permissions set to allow only the individual accounts or groups (roles) that require access to be able to connect.
- Permissions must be reviewed frequently enough to ensure appropriate access levels are being maintained and to prevent unauthorized access.

OS AND APPLICATION MAINTENANCE -- PATCHES: *(Required)*

- The system administrator is responsible for obtaining and reviewing information about relevant OS and application security issues, patches, and maintenance issues, and making decisions regarding the application of patches to their system.
- Critical, high-risk patches and service packs should be applied as soon as possible, and lower-risk patches and service packs should be applied within a reasonable period after they are released, as appropriate for the system.

OS AND APPLICATION MAINTENANCE – UPGRADES: *(Required)*

- Operating systems and applications must be maintained by the system administrator at the most recent stable version that is compatible with the system's hardware and function.
- If an older OS or application is required due to hardware or software functional restrictions, measures should be taken to limit access to the system (via host-based firewall, router access control, internal limitation of available services, or other measures) in order to reduce the risk of exploitation of old, non-repairable vulnerabilities.
- Operating systems and applications that cannot be upgraded must have the circumstances of the restriction documented in "Non-Compliant Device Waiver", which will also help evaluate other possible protections that could

be used. This waiver can be found on the Information Security webpage at http://infosec.uthscsa.edu/hsc_secpol/Waivers/waivers.html .

(Where Possible)

- Systems with operating systems or applications that cannot be upgraded due to hardware or functional restrictions should be removed from network access or replaced with newer systems.

SYSTEM LOGGING AND MONITORING: ***(Required)***

- OS event logging must be enabled for security events such as failed logins and unauthorized connections for any commonly used service.
- Application event logging should be used to record unauthorized access attempts and if possible to track configuration changes.
- Logs must be reviewed on a regular basis to monitor for suspicious activity in the OS, applications, or network.

(Where Possible)

- Logs on critical servers or those providing high-vulnerability services or hosting sensitive applications should be reviewed daily.
- Use of remote logging to a log server increases the chance that compromises will be caught because the logs on the remote server are generally safer from tampering by hackers.
- Log concentration and interpretation programs can be used to ease the task of reviewing logs and finding potential problems.

USER ACCOUNT MANAGEMENT: ***(Required)***

- All user accounts must be password authenticated or require a physical token or biometric authentication.
- Account creation and authorization processes must be based on the principle of least privilege, with access to systems granted only to those who require it on a need-to-know basis.
- Accounts must be reviewed regularly (minimum every 2 months). Accounts that are no longer needed (i.e. for an terminating or transferring employee) should be deactivated as soon as reasonably possible.
- Procedures must be in place for emergency termination of user accounts.
- User accounts should be individually assigned and maintained except in cases where an application, hardware, or function requires that a single common account be used.
- Unused accounts must be managed (locked and/or removed) in a timely manner to prevent misuse of old accounts by hackers or users who no longer have the authority to access the system.

(Where Possible)

- Many operating systems have mechanisms to set account attributes such as maximum inactivity period and authentication rules. Use these built-in mechanisms to simplify the process of monitoring and maintaining user accounts.

DEFAULT ACCOUNT MANAGEMENT: ***(Required)***

- Default OS or application accounts included by the manufacturer or used in installation of a system are sometimes left open when the system goes into use. System Administrators should research default accounts by referencing the OS or application documentation or by searching for the phrase "default password list" on the Internet.
- Default, backdoor accounts must be disabled or removed to prevent unauthorized access to the system.

(*Where Possible*)

- Default "administrator" accounts should be renamed in order to reduce the likelihood that a malicious user can guess the username and password for administrator-level accounts.

CONFIGURATION AND CHANGE MANAGEMENT: ***(Required)***

- Server configuration and changes made must be tracked and recorded in a way that allows the server administrator and related managers to understand what the current and future system configuration, network access, and data flow considerations may be.
- A configuration management process must be put into place that includes, at a minimum:

    - Initial server configuration and licensing
    - Changes as they are made
    - Tracking of hardware service and maintenance issues
    - Software and OS upgrade and maintenance
    - Testing plans and results for any changes that may impact usage or performance
    - Communication with users and others impacted by server changes

- Configuration management and change control processes must be appropriate for the data classification and criticality of the server, but can be scaled to fit department size and number of users affected. It must include a process for changes to be reviewed and approved by the data owners and/or departmental management.

PHYSICAL SECURITY: ***(Required)***

- All servers must be housed in non-public, limited-access areas with lockable doors.

- Critical systems and systems that contain sensitive information must be physically attached via a secure locking device to some relatively immobile object or housed in an area that uses access control systems (card-key, crypto-lock, etc.) or otherwise provides strictly controlled access (i.e. system administrator and police only).
- Uninterruptible Power Supply (battery backup) power protection should be sufficient to allow time to shut down the server in case of a power outage.
- Heating and cooling in the server area should be sufficient to maintain temperature and humidity within hardware tolerance ranges.
- The area around and on top of the server should be kept clear of debris, papers, supplies, manuals, and other items that might interfere with air circulation or proper function of the server.
- Do not store non-server-related items or supplies in a server area.

(Where Possible)

- Chassis locks or locking racks should be used where possible to prevent removal of internal components. Any chassis or hardware access keys must be stored in a secure location away from the server.
- Fire suppression systems other than the standard "wet pipe" sprinkler systems should be used in server rooms to mitigate the risk of fire damage to the server and to reduce the chance that equipment and data loss and/or personnel injury will occur due to sprinkler damage or malfunction.

MALWARE SCANNING AND REMOVAL: ***(Required)***

- All decentralized mail and file servers must provide malware scanning capability equivalent to or better than that used on centralized mail and file servers.
- Because of the high prevalence of malware targeting Microsoft Windows operating systems, all Windows-based servers are required to have malware scanners installed or be remotely scanned on a regular basis regardless of function, except where such installation or scanning would seriously compromise the server or threaten functionality.
- Exceptions to the scanning requirement must be approved and documented by waiver with the CISO.

(Where Possible)

- Malware scanning software is recommended for all servers regardless of operating system or function.

INTRUSION AND COMPROMISE DETECTION AND PREVENTION:
(Where Possible)

- Servers that contain sensitive information should have intrusion and compromise detection and prevention of some sort in place and regularly

monitored. Some examples of intrusion prevention products include host-based firewalls (IPFilter, ZoneAlarm, Symantec, etc.), change auditing software (such as TripWire), extended access control and auditing (such as TCPWrappers), or intrusion detection packages.

LOGIN BANNERS: ***(Required)***

- Either the long or short UTHSCSA-approved warning banner must be displayed anytime a user attempts to connect to an authenticated resource (login via telnet, ftp, ssh, https, etc.).
- The long banner should be used wherever possible, but devices that cannot handle strings longer than 256 characters can use the short version. For more information see http://infosec.uthscsa.edu/General/banners.html.

Exceptions

Any exceptions to this document must be reviewed and approved by the Information Security Office.

Definitions

NOTE: This definitions section will not be a permanent part of this standard, but will be transformed into a reference that will have required definitions for all of the standards and guidelines, and will be published separately on the InfoSec standards and guidelines web page. This section is left here currently for your reference and comments.

Public IT Resources: Any non-sensitive, generally available information that can be made available without the need for individual logins or other forms of authentication. Public IT resources can be either externally available (such as the UTHSCSA website and some departmental or study sites) or could be internal only (such as a departmental website with documents and information only for members of that department). Databases and other potentially sensitive or proprietary information are rarely public IT resources.

Non-Public IT Resources: Any IT resources that require a higher level of protection from exposure by user login or other authentication. These can also be either external (such as a study website that requires a login to access it) or internal (study websites, internal databases on servers, mapped shares, etc.)

Server: A server is any computer system connected to the UTHSCSA network that:

1) is a data processing device which has an assigned IP address within the University's static IP range and is capable of either multiple simultaneous connections or any remote connections to allow use or administration of the system, or

2) is a data processing device shown to be offering connectivity or services that are consistent with those that would be offered by a server (i.e. telnet, ftp, smtp, web pages, and others).

Printers and other peripheral devices with assigned static IP addresses are not servers, but desktop PC's (any OS) that host a web page or allow remote logins must be treated as servers, whether they have static IPs or not, because those services open the computer and the network up to some of the same threats as servers. Desktop computers offering shared directories and files will not be considered servers unless they are specifically designated as such by the owning department, because sharing issues are dealt with separately. Servers that reside on the UTHSCSA network but are fully or partially owned or managed by other institutions must still meet the server standard in order to remain on the network. Systems that reside on other institution's networks but are owned by UTHSCSA and used primarily for UTHSCSA-related functions are considered UTHSCSA servers and must comply with this standard except where it conflicts with established standards or functionality on the network where it resides.

Decentralized Server: Any server that is physically located outside of the UTHSCSA Central Computing Facility or is not administered by Computing Resources staff.