SERVER SECURITY

Policy

Definition

For the purpose of this policy, and all related policies and standards, a server is defined as a computer or computer application that provides access to centralized resources or services to other computers on a network. Server services include, but are not necessarily limited to, web services, mail services, database services, and file services. Desktop workstations are not authorized to provide server services as they are not likely to have the necessary physical and logical safeguards described in this policy and standard.

Data Centers and Domain Membership

All server computers must be established and maintained in a manner that provides physical and logical security sufficient to protect both the server hardware and the information it holds. As directed by the Health Science Center Executive Committee, all servers must be located in one of the approved University data centers. Exceptions to this requirement must be approved by the Vice President and Chief Information Officer.

Physical access, logical access, server maintenance, and data management may be negotiated with Systems and Network Operations through a server maintenance agreement from Client Support Services. The financial obligation for maintenance of a server resides with the department or division that claims ownership of the server or as specified in service level agreements.

To ensure proper reporting, patch management, malicious software prevention updates, and general accountability, all servers must be registered with the University’s active directory domain structure if they are capable of doing so. Exceptions to domain membership must be approved by the Chief Information security Officer (CISO). All requests for exceptions must be accompanied by a written business case and justification, approved by the department’s Dean, Director, or Chair.

Those servers identified outside of an approved data center without an exception or an action plan to move into a data center will have their
network access removed until such a time as an exception has been granted or an action plan has been approved. Similarly, identified servers that are not joined to the domain will have their network access revoked until they have either joined the domain or an exception has been granted.

Data Separation

Production/Test: To avoid inadvertent data disclosure, production and test/development servers must be maintained and operated in separate environments. Additionally, production data, especially any data of a sensitive nature, must never be used in the test/development environments. If a realistic data set must be used in a test/development environment, steps must be taken to render any production data unidentifiable while still maintaining proper structure and schema.

Sensitive/Non-sensitive: Every effort should be taken to minimize storage of sensitive and non-sensitive information on the same server or virtual instance. If both data types must be stored on the same device or instance, steps must be taken to protect the sensitive data commensurate with its sensitivity.

Server Administration

Any server in use at the Health Science Center must be managed by an administrator who is considered qualified by the Health Science Center’s Information Security Office (ISO) for security administration of that specific type of server. The ISO will recommend appropriate security training and qualification opportunities. This training will be applicable to those departments that intend to manage their servers in their own active directory organizational unit but still within a data center. The ISO will attempt to obtain no-cost or low-cost training, but departments will likely be required to fund individual training for their administrators.

Once security administration qualification is obtained for a particular type of server, the qualified administrator can become the registered security administrator for multiple servers of that same type, up to an amount that the administrator can reasonably be expected to manage. Active participation in the Health Science Center’s Technical Support Representative (TSR) program is a requirement for all server
Security administration training and qualification is limited to concepts associated with server security, and does not regulate administrator tasks or skills not related to security. The member of management with assigned ownership for the server is responsible for obtaining general server administration services from a competent administrator. Information regarding training for general server administration can be obtained with the assistance of the Technology Training Office of Client Support Services (CSS).

If the department that owns a server does not wish to designate or hire a qualified administrator, a server maintenance agreement contract for general server and/or security administration services can be arranged through CSS.

Should management choose not to accept the responsibilities for secure management of a server, and/or administration of the server is neglected in such a way that it becomes a threat to the security of other computers or the Health Science Center’s network, action will be taken to eliminate the threat by removing the server from network access. If this action is taken, the server will be ineligible to be reconnected to the network until a qualified administrator can be found.

Out-of-Date Operating Systems

Computers with obsolete and unsupportable operating systems must be removed from the network until such time as the operating systems can be upgraded or replaced with a supported version. Obsolete operating systems are those no longer being supported with upgrades, patches, or fixes; these versions represent a threat as vulnerabilities may be discovered which will not be fixed by the manufacturer. If a computer with an obsolete operating system is considered critical or necessary for a department but cannot be upgraded, steps must be taken to implement compensating controls so that the computer may remain in operation, including removal from the University network and/or blocking access to/from the Internet. Waivers for these and other legacy systems and non-compliant computers must be submitted to and approved by the Chief Information Security Officer, along with business cases from the appropriate dean, directory, or chair.
**Time Synchronization**

All servers must be configured to synchronize with the University’s time server to aid in investigations, for incident management, and for system log reviews.

**Compliance**

All servers must comply with all applicable policies, laws, rules and regulations, including the Health Science Center’s *Server Security Standard*. This standard, as well as other security standards and guidelines pertaining to information security policies, may be found at the Information Management and Services web site ([http://ims.uthscsa.edu/policies.aspx](http://ims.uthscsa.edu/policies.aspx)).

**Accountability**

**Departmental**

Deans, Chairs, and Directors are accountable for ensuring that their department remains in compliance with all applicable local, state, and federal information security policies as described in the HOP, Section 4.9.2, “Management’s Responsibilities”. If it is determined that the University’s network, systems, data, or mission have been put at risk due to a willful or negligent lack of compliance with information security policies, Information Management and Services (IMS) personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, IMS is authorized to assess the department a service fee for security remediation and/or reconnection of services. The service fee will be charged to the department’s state funds account.

**Individual**

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2, “Handbook of Operating Procedures”.