



Handbook of Operating Procedures

Section:

8.9.4

Originally Approved:

01/25/02

Last Amended:

SERVER MANAGEMENT POLICY

A. Purpose

The purpose of this policy is to provide for the appropriate management of university servers; enhance the security of the servers against intrusion and misuse, enhance protection of the university network and other information resources from attacks; and provide those responsible for servers with a basic set of guidelines to achieve proper management.

B. Authority and Requirements

1. University of Texas System Guidelines BPM 53 and the Texas Department of Information Resources (DIR) "Information Security and Risk Management Policy Standards and Guidelines" as published in the *Texas Administrative Code* 1 TAC 201.13(b) and as authorized by the *Texas Government Code*, Chapter 2054.
2. University of Texas-Pan American 8.9.1, Policy for the Use and Protection of Information Resources; 8.9.2, Computer and Information Technology Use Policy; and 5.5.2, Student Code of Conduct as published in the *Handbook of Operating Procedures*.

C. Definition

A server is a computer specifically configured to communicate through a network and provide a service to one or more individuals. A server is a University Server when it is connected to the campus network by any means and uses a UTPA Internet address. Server management involves controlling user access, setting/maintaining security measures in place and monitoring server configuration and performance.

D. Scope

This policy applies to all owners, custodians, and technical managers of servers. This policy applies to all university servers as defined in C above, including those residing on personally owned hardware.



Handbook of Operating Procedures

Section:

8.9.4

Originally Approved:

01/25/02

Last Amended:

SERVER MANAGEMENT POLICY

E. Statement of Policy

The owner of a server is responsible for the management, operation and security of the server. At a minimum, the owner must assure the server is physically secured, electronic access to the server is properly controlled, and server configuration is maintained within specified security parameters. The owner may delegate management responsibility for the server to a custodian or technical manager. The assigned custodian or technical manager is responsible to the owner for the actions of both the server and server users. The owner of a server may have to place additional requirements beyond the scope of this policy to achieve mandated regulatory compliance and to protect any designated private, confidential, sensitive, or otherwise protected information maintained or archived in the server.

F. Responsibilities

1. General responsibilities regarding University server management are outlined below:
 - a. Owner: The owner insures anyone assigned to manage a server is qualified to perform technical duties, has adequate back up, and receives resources necessary, including appropriate training or instruction, to comply with the requirements of this and other policies.
 - b. Custodian: The custodian administers, controls and configures servers in compliance with the requirements of the owner and policies in force.
 - c. Technical Manager: The technical manager is assigned by the resource owner or custodian to manage server(s). The assigned technical manager shall attain and maintain knowledge and expertise equivalent to the scope of assigned responsibilities and systems supported.

G. Minimum Server Management Requirements

1. **Server Requirements:** Requirements for servers are outlined below. Additional requirements apply for special servers that process and/or store mission critical or confidential information. Resource owners may place additional requirements on their servers as deemed necessary.



Handbook of Operating Procedures

Section:

Originally Approved:

Last Amended:

8.9.4

01/25/02

SERVER MANAGEMENT POLICY

- a. All Servers - A server may be connected to UTPA Campus Network if it complies with the following minimum technical and security requirements:
 - 1) The system must run an appropriately licensed version of an operating system that supports appropriate Internet communication protocols.
 - 2) The server must run only necessary services. After it has been determined what services are needed, all unnecessary services should be shut down.
 - 3) The server must have all default account passwords changed and after determining what default accounts are required, have all other default accounts disabled.
 - 4) The server must have the latest system patches applied regularly, normally within thirty days. Although promptly loading the most recent version of operating systems is not required, it is required to promptly apply all security patches, service packs, or hot-fixes to the operating system that have been released.
 - 5) The server must authenticate all users to ensure only authorized users can access the resource. Supplementary authentication mechanisms should be considered for systems that process or store mission critical or confidential information.
 - 6) The server must enforce password policy including requiring periodic password changes for all users (no less than once per year) and denying login after a specified number of failed login attempts.
 - 7) The server must have all old user accounts terminated promptly (normally within five working days). A clear deadline must be established for account termination of persons no longer affiliated with the University.
 - 8) The server must have virus protection software installed and maintained current.
 - 9) The server must capture and archive critical user, network, system and security event logs to enable review of system data for forensic and recovery purposes.



Handbook of Operating Procedures

Section:

Originally Approved:

Last Amended:

8.9.4

01/25/02

SERVER MANAGEMENT POLICY

- 10) The server mail system must create return addresses with the correct Internet host/domain address and must recognize its own address and accept mail destined for users at that server.
 - 11) The server may not function as a relay for SMTP or other means of relaying non-University related email.
- b. Special Servers – In addition to above server requirements, the following requirements apply to special servers that process or store mission critical or confidential information.
- 1) The server must not be used for inappropriate functions such as testing applications or research and development.
 - 2) The server must maintain a password history to prevent the reuse of recent passwords, and should be capable of testing user passwords for easy guessing (dictionary words, common acronyms, etc.).
 - 3) The server must be either physically secured or have appropriately installed software or hardware devices to safeguard against inappropriate access from/to the Internet and prevent unauthorized access, theft, and destruction.
 - 4) The server must have a limited number of user accounts with administration privileges and should have several file and access categories defined and used to prevent excess user privileges.
 - 5) The server must not use a dial-in/dial-out modem for remote access unless specifically approved by the server owner.
 - 6) The server must have file backup tools and devices installed and used to periodically archive user and system data.
 - 7) The server should encrypt remote administration traffic and should accept remote administration commands only from an authenticated administrator and only from one particular host.



Handbook of Operating Procedures

Section:

8.9.4

Originally Approved:

01/25/02

Last Amended:

SERVER MANAGEMENT POLICY

H. Policy Violations

Violations of this policy may result in the following:

1. A server discovered to have been compromised or breached, and that has been determined to be improperly managed during forensic analysis, may be removed from the campus network until security configuration upgrades have been completed.
2. Those responsible for the violation(s) may be subject to any or all the administrative and disciplinary processes outlined in applicable operating policies and procedures of the University.

I. Review

This policy shall be reviewed every four years by the University's designated Information Resources Manager.