

# TSUS Policy Guideline

**TSUS Policy Guideline:** Server Management Policy

**Policy Guideline ID:** TSUS IT.04.01

**Approval Authority:** TSUS Board of Regents

**Approval Date:**

**Effective Date:**

**Next Review Date:**

## **Purpose/Reason**

The Texas State University System (TSUS) considers information technology to be a critical enabler in meeting its mission and has made significant investments in information technology assets and capabilities. The Texas State University System recognizes the inherent value of these information technology resources to the state, the System, and their constituents. Likewise, Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202) underlines the importance of information technology resources residing in Texas public higher education institutions by requiring state institutions “to protect these assets against unauthorized access, disclosure, modification or destruction,” and “to assure the availability, integrity, utility, authenticity, and confidentiality of information.” Compliance with this policy contributes to the availability, protection, and appropriate use of the information technology resources of the Texas State University System and its component institutions.

## **Policy Statement**

The Texas State University System and its component institutions must ensure the confidentiality, integrity, reliability, and availability of their server hardware and software to fulfill their institutional missions and to assure compliance with the management and security standards for public institutions of higher education described in TAC 202. To guide institutional policies related to the management and use of institutional servers, the Texas State University System has set forth the following specific topics and provisions to be incorporated into each institution’s specific policy statement on server management. Thus, each component institution shall develop and disseminate an institutional policy statement on server management that is consistent with TAC 202 and the specific topics and provisions described below.

## **Policy Specifics**

The following specific topics and objectives must be addressed by institutional server management policies.

### **1. Server Purpose and Function**

Objective: To assure the suitability of the server and its connection to the institutional network. The institutional network is a state information resource that exists to achieve the mission, goals, and objectives of the institution. The purpose and function of any server connected to the institutional network must also be consistent with and in support of institutional initiatives.

### **2. Server Management Roles and Responsibilities**

Objective: To assign responsibility and accountability for management of the server hardware, software, and data. A management framework should be defined that clearly delineates the roles and responsibilities for management of the server. At a minimum, distinct roles should be delineated for a server owner and a server administrator. Owners are typically responsible for establishing server usage policies, specifying server access controls (both physical and electronic), and assuring compliance with state and institutional server management standards. Administrators are typically responsible for enforcing the owner’s usage policies, implementing the owner-specified access controls, and configuring the server according to the required standards.

### **3. Conformance with Server Management Best Practices**

Objective: To assure that all server owners and administrators adhere to documented standards and best practices for server management. An institutional guide to server management standards and best practices should be made available to all server owners and administrators. Compliance review procedures should be established and exceptions should be justified by documented risk management decisions. At a minimum, the guide should address the following topics:

## TSUS Policy Guideline

- A. Licensing, support, and update management for the operating system and all hosted services and applications
- B. Automated threat mitigation (e.g., anti-virus software, host-based firewall, etc.)
- C. Protection for any sensitive and confidential data accessible via the server
- D. Disablement of prohibited, unauthorized, and unnecessary services
- E. Disablement and/or modification of default and unnecessary accounts and passwords
- F. Physical and electronic access controls that support role-based access, appropriate separation of duties, and the principle of “least privilege”
- G. Backup and recovery
- H. User authentication
- I. Activity and event logging
- J. Network connection requirements and standards (e.g., server registration)

#### 4. Threat and Incident Response

Objective: To set expectations regarding the disconnection or isolation of threatening servers. Servers that pose an immediate threat to network operations, performance, or other network-connected devices must be disconnected or quarantined to minimize risk until the threat is removed. Incident response best practices must be followed to assure appropriate preservation and treatment of forensic data.

#### Scope and Applicability

This policy guideline applies to all persons and organizations that manage or utilize information technology resources belonging to the TSUS or any of its component institutions.

#### Definitions

**Information Technology Resources** - any of the following that are owned or supplied by the TSUS or one of its component institutions: usernames or computer accounts, hardware, software, communication networks and devices connected thereto, electronic storage media, related documentation in all forms. Also included are data files resident on hardware or media owned or supplied by the TSUS or a component, regardless of their size, source, author, or type of recording media, including e-mail messages, system logs, web pages and software.

**Server** – A network device that performs a specific service or function on behalf of other network devices or users.

**Server Administrator** – The individual designated by the server owner as responsible for performing server management functions.

**Server Management** – Functions associated with the oversight of server operations. These include controlling user access, establishing/maintaining security measures, monitoring server configuration and performance, and risk assessment and mitigation.

**Server Owner** – The department head charged with overall responsibility for the server asset in the university’s inventory records. The server owner must designate an individual to serve as the primary system administrator and may designate a backup system administrator.

#### Authority and Responsibility

Questions related to this policy guideline or to the server management policy statement at any component institution should be addressed to the Chief Information Officer at the component institution.

#### Additional background, Related Policies, and other References

In addition to the general guidelines set forth in this document, server management policies may be affected by a number of other legal requirements and ethical principles. While it is not possible to list all potentially applicable laws and regulations, the following are particularly likely to have implications for information security policies:

1. The federal Family Educational Rights and Privacy Act (commonly known as FERPA) - restricts access to

## TSUS Policy Guideline

personally identifiable information from students' education records.

2. Texas Administrative Code, Title 5, Subtitle A, Chapter 552: The Texas Public Information Act (formerly known as the Texas Open Records Act) – provides that all information collected, assembled, or maintained by governmental bodies is public information and available to the public during normal business hours, unless the information falls within certain exceptions specified in the Act.
3. Texas Administrative Code, Title 1, Part 10, Chapter 202 - Regulations from the Department of Information Resources establishing requirements for State agencies regarding information resources security.
4. Texas Penal Code, Chapter 33: Computer Crimes - Texas law pertaining to computer crimes. This statute specifically prohibits unauthorized use of University computers, unauthorized access to stored data, or dissemination of passwords or other confidential information to facilitate unauthorized access to the University's computer system or data.
5. Texas Penal Code, § 37.10: Tampering with Governmental Record - Prohibits any alteration, destruction, or false entry of data that impairs the validity, legibility or availability of any record maintained by the University.
6. United States Code, Title 18, § 1030: Fraud and Related Activity in Connection with Computers - Federal law specifically pertaining to computer crimes. Among other stipulations, prohibits unauthorized and fraudulent access to information resources.
7. Computer Fraud and Abuse Act of 1986 (Part of 18 U.S.C. § 1030) - Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.
8. The Computer Abuse Amendments Act of 1994 (Part of 18 U.S.C. § 1030) - Expands the Computer Fraud and Abuse Act of 1986 to address the transmission of viruses and other harmful code.
9. Federal Copyright Law - Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.
10. Digital Millennium Copyright Act - Signed into law on October 20, 1998, as Public Law 105-304. Created to address the digitally networked environment, the DMCA implements the WIPO Internet Treaties; establishes safe harbors for online service providers; permits temporary copies of programs during the performance of computer maintenance; and makes miscellaneous amendments to the Copyright Act, including amendments that facilitate Internet broadcasting.
11. Electronic Communications Privacy Act of 1986 - Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.
12. Computer Software Rental Amendments Act of 1990 - Deals with the unauthorized rental, lease, or lending of copyrighted software.
13. Texas Government Code § 556.004 - Prohibits using state resources or programs to influence elections or to achieve any other political purpose.
14. Health Insurance Portability and Accountability Act – Public Law 104-191, August 21, 1996. The final standards were published in February, 2003 and emphasize security management principles and broad management controls as primary vehicles for protecting patient health information.
15. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, Public Law 107-296. Provides a framework for ensuring the effectiveness of information security controls over information

## TSUS Policy Guideline

resources that support Federal operations and assets.

Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of the institution's information technology resources.

DRAFT