

TSUS Policy Guideline

TSUS Policy Guideline: Network Management Policy

Policy Guideline ID: TSUS IT.03.01

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.” TAC 202 also stipulates that “access to state information resources must be appropriately managed.” Compliance with this policy guideline contributes to the availability, protection, management and appropriate use of the data, voice, and video networks 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 data, voice, and video networks 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 networks, 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 network management. Thus, each component institution shall develop and disseminate an institutional policy statement on network 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 network management policies:

1. Network Purpose

Objective: To affirm the purpose of the institutional network. The institutional network is a state information resource that exists to achieve the mission, goals, and objectives of the institution. Utilization of the network must be consistent with and in support of institutional initiatives.

2. Network Address and Device Management

Objective: To assure appropriate oversight over the connection of devices to the institutional network. The integrity, security, and proper operation of the network require an orderly assignment of network addresses and the correct configuration of devices attached to the network. Network access, performance and security are put at risk when devices are introduced into the network environment without appropriate planning and coordination. All devices acting in the role of a server (regardless of their specific function, hardware, or software) must have a designated device administrator and must be registered in a network device registry administered by the institution’s Information Resource Manager (IRM) or designee.

3. Network Management Roles and Responsibilities

Objective: To assign responsibility and accountability for management of the institutional network. A management framework should be defined that clearly delineates the roles and responsibilities for management of the institutional network. Institutional networks should be centrally administered by the institutional IRM (or designee) to assure consistency and compliance with the state’s network administration standards and best practices.

TSUS Policy Guideline

4. Network Usage Responsibilities

Objective: To delineate the responsibilities of network users and device administrators. Users and administrators of network-connected devices must understand their accountability for device management practices that might result in damage or harm to network operations, performance, or other network-connected devices.

5. Threat and Incident Response

Objective: To set expectations regarding the disconnection or isolation of threatening devices or networks. Devices or network addresses 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. Sources of repeated threats should be isolated for longer periods of time as required to permanently eliminate the threat.

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

Device - Any hardware component involved with the processing, storage, or forwarding of information making use of the Texas State information technology infrastructure or attached to the Texas State network. These devices include, but are not limited to, laptop computers, desktop computers, servers, and network devices such as routers, switches, wireless access points, and printers.

Device Administrator - An individual with principal responsibility for the installation, configuration, registration, security, and ongoing maintenance of a network-connected device.

Device Owner – The department head charged with overall responsibility for the networking component in the university's inventory records. The device owner must designate an individual to serve as the primary device administrator and may designate a backup device administrator. All network infrastructure devices, (e.g., network cabling, routers, switches, wireless access points, and in general, any non-endpoint device) shall be centrally owned and administered

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.

Institutional Network - the data transport and communications infrastructure at the institution. It includes the campus backbone, local area networks, and all equipment connected to those networks (independent of ownership).

Network Address - A unique number associated with a device used for the routing of traffic across the Internet or another network. Also known as Internet Protocol Address or IP Address.

User - An individual who uses an information technology resource, such as the institutional network or any network-connected device.

Authority and Responsibility

Questions related to this policy guideline or to the network 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, network 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 network management policies:

TSUS Policy Guideline

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

TSUS Policy Guideline

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 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