

TSUS Policy Guideline

TSUS Policy Guideline: Information Security Policy

Policy Guideline ID: TSUS IT.02.01

Approval Authority: TSUS Board of Regents

Approval Date: ITTF Approval Received October 19, 2007

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, and availability of their information technology resources to fulfill their institutional missions and to assure compliance with the security standards for public institutions of higher education described in TAC 202. Thus, each component institution shall develop and disseminate an institutional policy statement on information security consistent with TAC 202 and utilizing the following resources as guidelines:

- International Standardization Organization (ISO)/International Electrotechnical Commission (IEC) 17799:2005(E) (to be updated and renumbered as ISO/IEC 27002 in 2007) and
- The ongoing work of the EDUCAUSE/Internet2 Computer and Network Security Task Force.

Policy Specifics

The specific topics and objectives to be addressed by institutional information security policies are outlined below.

1. Information Security Policy

Objective: To have management provide clear direction and strong support for the institution’s information security program. Management should affirm its support for the information security policies, roles, practices and other program components necessary to achieve security, consistent with business requirements, relevant laws, and regulations.

2. Information Security Organization:

Objective: To effectively manage and execute the information security program within the campus. A management framework should be defined that clearly delineates the roles and responsibilities for management of information security within the campus.

3. Risk Assessment

Objective: To identify, quantify, and prioritize risks to the organization and its information assets. Risk assessment results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls to protect against these risks.

4. Information Asset Management

Objective: To achieve and maintain appropriate protection of campus information assets. Assets should be classified according to their need for security protection. Owners should be identified for all assets, and the responsibility for the maintenance of appropriate controls should be assigned.

TSUS Policy Guideline

5. Human Resources Security

Objective: To ensure that employees, contractors and other users understand their information security responsibilities and to reduce the risk of theft, fraud or misuse of information resources. Employees, contractors, and other users should be fully apprised of their security responsibilities. Their access to information assets should be managed consistent with their current institutional status, roles, and qualifications. Information security training should be provided to employees at new employee orientation and annually thereafter.

6. Physical and Environmental Security

Objective: To prevent unauthorized physical access, damage, and interference to the institution's information infrastructure, premises and information. Critical or sensitive information processing facilities should be housed in secure areas and protected from unauthorized physical access by defined security barriers and entry controls. They should be protected against loss from environmental threats commensurate with the identified risks and their importance to the institution's mission critical business processes.

7. Communications and Operations Management

Objective: To ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be defined. This includes the development and documentation of appropriate operating procedures.

8. Access Control

Objective: To control access to informational assets following the principle of least privilege. Access to institutional information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access privileges should be restricted to those required for performance of specific assigned roles.

9. Information Systems Acquisition, Development, and Maintenance

Objective: To ensure that security is an integral part of information systems management. Security requirements should be identified, agreed upon, and addressed in all phases of information systems administration, from procurement and development through implementation and ongoing maintenance.

10. Information Security Incident Management

Objective: To ensure information security events and weaknesses associated with information systems are managed in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures should be established and documented.

11. Business Continuity Management

Objective: To protect critical business processes and activities from the effects of major information system failures or environmental disruptions and to ensure their timely resumption. A business impact analysis and continuity management process should be developed to minimize the impact on the organization and to assure an acceptable level of recoverability.

12. Compliance

Objective: To avoid breaches of any law, regulation, contractual obligation, or institutional policy. Information resources should be regularly tested and audited to assure adherence with both external and internal standards.

Scope and Applicability

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

TSUS Policy Guideline

Definitions

Information Technology Resources include 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.

Authority and Responsibility

Questions related to this policy statement or to the appropriate use 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 policy statement, information security 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 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;

TSUS Policy Guideline

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 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.