Computer and Network Security

Original Implementation: January 24, 1995
Last Revision: November 2, 2015

This policy establishes the conditions and security requirements for the use of computing equipment and networks at Stephen F. Austin State University (SFA). Computing equipment includes desktops, laptops, servers, handheld devices, and printers. In order to comply with state requirements (Information Resources Management Act, Tex. Gov't Code Ch. 2054, and Tex. Admin. Code, Title 1, Part 10, Ch. 202), the chief information officer serves as the information resources manager for the university.

Definitions:

Information Technology (IT) Security Sensitive Positions – Employees with application security permissions allowing access to information other than their own personal employee information.

Scope:

This policy applies at all university locations or data centers and represents the minimum requirements that must be in place. Individual areas with computers and networks may have additional controls and security.

Policy:

1. Each vice president, dean or director will designate staff (not student employees) or the technical services group of Information Technology Services (ITS) as responsible for the support, maintenance and security of the computing equipment within their purview. For organizational units that designate local staff as their support provider, ITS will provide computing support guidelines specifying the level of support that ITS will provide as the secondary support provider.
2. Each organizational unit will implement local security procedures to include:
    a. Protection of the privacy of confidential information;
    b. Protection of information against unauthorized modification;
    c. Protection of systems against unauthorized access and use;
    d. Display of the security banner from the ITS security web page on organization computers;
    e. Use of the university's central authentication source for user authentication on servers and desktop computers, where feasible;
    f. Use of the standard university antivirus software in a managed configuration, where feasible.

3. Each organizational unit of SFA that maintains a local area network(s) must develop a local security procedures document that is subject to approval by ITS. In order to mitigate and manage risk, each organizational unit maintaining servers will participate in the annual information systems security risk assessment. The president or designee will make the final security risk management decisions either to accept exposures or to protect the data according to their value or sensitivity.
4. SFA will not be liable for the loss of data or interference with files resulting from the university's efforts to maintain the privacy and security of the university's computer, information, and network facilities. In order to maintain network security, the university reserves the right to:
    a. Limit, restrict, or terminate an account holder's usage;
    b. Inspect, copy, remove, or otherwise alter any data, file, or system resource that threatens the security of a system or network, with or without prior notice to the user;
    c. Check systems periodically and take the necessary actions to protect university computers, information, and networks.
5. Individuals will exercise responsible, ethical behavior when using the university's information resources. The university reserves the right to limit, restrict or extend privileges and access to its resources.
    a. Access to certain university information resources is provided through the establishment of an account. Computer accounts must be approved in writing through the respective dean or director (or designated representative) of the administrative unit.
    b. Since the university permits access to copyrighted data through the Internet, each user is responsible for complying with university policy 9.3, Digital Millennium Copyright. Disciplinary action, including termination of service, may be taken on any reported copyright infringements that have been investigated and determined valid.
    c. Computer systems provided by SFA are reserved only for university-related activities (See Chapter 39 of the Texas Penal Code for provisions dealing with the misuse of state property). The intentional deletion or alteration of information or data of others, intentional misuse of system resources, and misuse of system resources by others are prohibited.
6. All employees will have security awareness training commensurate with their role at the university. All employees in IT Security Sensitive Positions must complete security awareness training annually. Each department head or academic unit head is responsible for ensuring employees are correctly identified as being in IT Security Sensitive Positions and the employees identified participate in security awareness training.
7. Each user is responsible for complying with university policies 16.32, Use of Electronic Information Resources and 9.1, Computing Software Copyright.

Sanctions for Policy Violations:

Violations of any provision of this policy may result in, but are not limited to:

a. a limitation on a user's access to some or all university computer systems;
b. the initiation of legal action by the university;
c. restitution by the violator for any improper use of service; and/or
d. disciplinary sanctions, which may include dismissal.

Many academic courses and work-related activities require the use of computers, networks, and systems of the university. In the event of an imposed restriction or termination of access to some or all university computers and systems, a user enrolled in courses or involved in computer related work activities may be required to use alternative facilities. However, users are advised that if alternative facilities are unavailable or not feasible, users are responsible for the failure to complete requirements for course work or work responsibilities.

Cross Reference: Use of Electronic Information Resources (16.32); Computing Software Copyright (9.1); Digital Millennium Copyright (9.3); Texas Information Resources Management Act, Tex. Gov't Code Ch. 2054; 1 Tex. Admin. Code §§ 202.1-.2, .70-.76; Tex. Penal Code §§ 39.01-.02.

Responsible for Implementation: Provost and Vice President for Academic Affairs

Contact for Revision: Chief Information Officer

Forms: None

Board Committee Assignment: Academic and Student Affairs