# 7.04 APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES
(Effective 02/1/2009)

**Modeled after TSUS Policy Guideline:** Appropriate Use of Information Technology Resources
**Policy Guideline ID:** TSUS IT.01.01
**Draft Date:** 12.23.2008
**Approval Date:** 01.22.2009
**Effective Date:** 02.01.2009
**Next Review Date:** 01.01.2011

## Purpose/Reason

Sul Ross State University (SRSU) considers information technology as a critical enabler in meeting its mission and has made significant investments in information technology assets and capabilities. Likewise, Texas Administrative Code, Chapter 202, Subchapter C, describes the information technology resources residing in Texas public higher education institutions as "strategic and vital assets belonging to the people of Texas" and that these resources must be managed "commensurate with their value" in a fashion that assures their protection and availability for appropriate use by authorized individuals. Compliance with this policy contributes to the availability, protection, and appropriate use of the information technology resources of Sul Ross State University and its component institutions.

## Policy Statement

It is the policy of Sul Ross State University to afford broad access to information technology resources by students, faculty and staff for activities that are related to, support, and fulfill institutional missions.

## Policy Specifics

**1. Institutional vs. Individual Purpose**

Access to information technology resources carries with it the responsibility for ensuring that the use of these resources is primarily for institutional purposes and institution-related activities, and for maintaining the integrity and security of the institution's computing facilities. In the interest of making the use of information technology resources a natural part of the day-to-day work of all members of the institutional community, incidental personal use is tolerated. However, employees are not to use any information technology resources in an extensive or regularly recurring manner for activities that are unrelated to institutional purposes. Individuals with authorized access to information technology resources must ensure that their access permissions are not accessible to, transferable to, or usable by any other individuals.

**2. Personal vs. Official Representation**

Information technology resources are a dynamic mechanism for the free exchange of knowledge. It is desirable for SRSU to foster the robust dialogue that results from the use of the resources and to encourage students, faculty and staff to participate in that dialogue. Those exchanges that reflect the ideas, comments and opinions of individual members of the SRSU community must, however, be distinguished from those that represent the official positions, programs and activities of SRSU. Students, faculty and staff using information technology resources for purposes of exchanging, publishing or circulating official institutional documents must follow institutional requirements concerning appropriate content and style. SRSU is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet or world wide web, that reflect only the personal ideas, comments and opinions of individual members of the SRSU community, even where they are published or otherwise circulated to the public at large by means of SRSU information technology resources.

**3. Limitations on the Availability of Information Technology Resources**

Sul Ross State University's information technology resources are finite by nature. All members of the SRSU community must recognize that certain uses of institutional information technology resources may be limited or regulated as required to fulfill SRSU's primary teaching, research and public service missions. Examples of these limitations include those related to capacity management, performance optimization, or security of the institution's information technology systems.

**4. Privacy and Confidentiality of Electronic Documents**

No information technology system can absolutely guarantee the privacy or confidentiality of electronic documents. More importantly, information technology resources provided by SRSU are essentially owned by the State of Texas and subject to state oversight. Consequently, persons that use these state-owned resources or any personally owned *or third party device that may be connected to a state-owned resource*, have no right to privacy in their use of these resources and devices. SRSU will, however, take reasonable precautions to protect the privacy and confidentiality of electronic documents and to ensure persons using SRSU information technology resources that the institution will not seek access to their electronic messages or documents without their prior consent except where necessary to:

- Satisfy the requirements of the Texas Public Information Act, or other statutes, laws or regulations;
- Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
- Protect the integrity of the institution's information technology resources, and the rights and other property of the institution;
- Allow system administrators to perform routine maintenance and operations, security reviews and respond to emergency situations; or
- Protect the rights of individuals working in collaborative situations where information and files are shared.

**5. Enforcement and Recourse**

- The University considers any violation of acceptable use principles or guidelines to be a serious offense, and reserves the right to test and monitor security, including copying and examining any files or information resident on university computer systems allegedly related to unacceptable use.
- Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network in any way is subject to immediate disconnection from the University's network. The CIO or designee may require specific security improvements where potential security problems are identified.
- Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. This includes but is not limited to attaching unregistered devices to the network; sharing passwords; leaving systems unattended that are logged into security sensitive servers; unauthorized monitoring of the network; and assisting someone else or requesting someone else to circumvent security or administrative access controls.
- Persons responsible for policy violations are subject to action in accordance with student, faculty and staff disciplinary policies and procedures and possible prosecution from local, state and federal authorities.
- To preserve and protect the integrity of information technology resources, there may be circumstances where SRSU must immediately suspend or deny access to the resources. Should an individual's access be suspended under these circumstances, the institution shall strive to inform the individual in a timely manner and afford the individual an opportunity to respond. The institution shall then determine what disciplinary action is warranted and shall follow the procedures established for such cases.

## Scope and Applicability

This policy statement applies to all persons and organizations that manage or utilize information technology resources belonging to Sul Ross State University.

## Definitions

**Information Technology Resources** include any of the following that are owned or supplied by Sul Ross State University: 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 SRSU 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 should be addressed to the Chief Information Officer or a member of the SRSU Executive Committee.

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

In addition to the general principles set forth in this policy statement, the use of information technology resources 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 the use of institutional information technology resources:

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.

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 Sul Ross State University's information technology resources.