SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Information Security Policy
SRSU Policy ID: APM 7.01
Policy Reviewed by: Chief Information Officer
Approval Authority: Executive Cabinet
Approval Date: 7-23-2013
Next Review Date: 7-23-2015

Purpose/Reason

Sul Ross State University (SRSU) considers information technology to be a critical enabler in meeting its mission and has made significant investments in information technology assets and capabilities. SRSU recognizes the inherent value of these information technology resources to the state, the Texas State University 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 Sul Ross State University.

Policy Statement

It is the policy of Sul Ross State University to ensure the confidentiality, integrity, and availability of our information technology resources to fulfill our institutional mission.

Policy Specifics

1. Information Security Policy

Objective: To have management provide clear direction and strong support for the institution's information security program.

SRSU's Executive Committee and CIO approve and support the security policies, roles, and practices necessary to achieve security consistent with business requirements, relevant laws and regulations. All individuals are accountable for their use of SRSU information resources and required to comply with applicable laws and university policies.

2. Information Security Organization:

Objective: To effectively manage and execute the information security program within the campus.

The Sul Ross Information Security Program is positioned within the Office of Information Technology and administered by the SRSU Information Security Officer (ISO) in collaboration with the Chief Information Officer (CIO) to whom the ISO reports.

The CIO meets weekly with the University's Executive Committee, which includes in its membership the University's designated Information Resource Manager (IRM), providing frequent opportunity to review any Information Security issues related to operations, process, policy, or incidents. The Executive Committee fully supports the SRSU Information Security Program.

The CIO and the ISO meet regularly with individuals responsible for campus information technology infrastructure and data resources. These forums provide frequent opportunities to address open issues and improve process.

3. Risk Assessment

Objective: To identify, quantify, and prioritize risks to the organization and its information assets.

SRSU uses risk assessment results to guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls to protect against these risks. SRSU utilizes a number of scanning and monitoring technologies, both externally and internally, to support risk identification, risk assessment, and remediation of identified risks.

4. Information Asset Management

Objective: To achieve and maintain appropriate protection of campus information assets.

To protect campus information assets, SRSU utilizes a threat matrix formula to classify assets according to their business purpose, and appropriate controls and maintenance duties are assigned.

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.

SRSU employees, contractors and other users are apprised of their security responsibilities. All SRSU OIT positions are classified as security sensitive and background checks are mandatory. Data owners for sensitive resources are clearly defined and they, in turn, have responsibility for designating authorized users of that data and their corresponding level of access.

6. Physical and Environmental Security

Objective: To prevent unauthorized physical access or damage to, or interference with, the institution's information infrastructure environment and information.

SRSU's critical and sensitive information processing facilities are housed in locked facilities and unauthorized access is forbidden.

7. Communications and Operations Management

Objective: To ensure the correct and secure operation of information processing facilities.

SRSU has defined responsibilities and procedures for the management and operation of all information processing facilities to be under the auspices of the Office of Information Technology. That office has assigned specific responsibilities and roles to appropriate members of its staff.

8. Access Control

Objective: To control access to informational assets following the principle of least privilege.

SRSU grants access privileges to its information processing assets only to SRSU employees, contractors and other users who require this access to fulfill their duties to the university. The level of access granted is determined by the data owners in consultation with OIT.

9. Information Systems Acquisition, Development, and Maintenance

Objective: To ensure that security is an integral part of information systems management.

Security requirements are identified, agreed upon, and addressed in all phases of information systems administration, from procurement and development through implementation and ongoing maintenance, as appropriate. Significant purchases undergo procurement review by SRSU Purchasing and SRSU Executive Committee.

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.

SRSU utilizes several logging and notification tools that monitor and automatically log or report to OIT staff several levels of events. SRSU Office of Information Technology staff report events and escalation procedures. SRSU maintains varying degrees of event reporting and formal reporting to the Texas Department of Information Resources and other state and federal agencies are used when appropriate.

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.

SRSU maintains a Business Continuity Plan to minimize impact on the organization and ensure an acceptable level of recoverability in the event of catastrophic failures of environmental or information systems.

12. Compliance

Objective: To avoid breaches of any law, regulation, contractual obligation, or institutional policy.

SRSU regularly audits and tests our network and information system resources using industry recognized tools and contracted services. IRM, CIO, and ISO monitor relevant notifications and updates from TSUS and DIR regarding these topics.

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.

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; 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.