SRSU Policy: Security Planning Policy
SRSU Policy ID: APM 7.33
Policy Reviewed by: Office of Information Technology
Approval Authority: Executive Cabinet
Approval Date: May 14, 2024
Next Review Date: May 14, 2029

Purpose: The purpose of this policy is to define information security controls around security planning.

Scope: This policy applies to Sul Ross State University. All users 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 resources.

Application: The statements in this document meet the minimum requirements established for the Texas State University System and its component institutions. At the discretion of Sul Ross State University, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the Sul Ross State University information security officer and appropriate Office of Information Technology staff.

POLICY/PROCEDURE

1. Policy Statements

1.1 Security planning procedures implemented by Sul Ross State University must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Sul Ross State University defines technical policy terms in the information technology glossary.

3. Security Planning Policy
Authority - DIR Controls Catalog (CC): PL-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of security planning policy and associated security planning controls; and

3.1.2 Review and update security planning procedures at an institution-defined frequency.

4. System Security Plan
Authority - DIR CC: PL-2

4.1 Each Information System under the custodianship of Sul Ross State University must have a corresponding System Security Plan that:

4.1.1 Is consistent with the university's enterprise architecture;

4.1.2 Describes the function and security posture of the information system;

4.1.3 Provides the security categorization of the information system, including supporting rationale;

4.1.4 Describes the operational environment for the information system and relationships with or connections to other information systems;

4.1.5 Provides an overview of the security requirements for the system that identifies the security controls in place;

4.1.6 Identifies any relevant institution-defined overlays, if applicable; and

4.1.7 Is reviewed and approved by the information owner prior to plan implementation.

4.2 Copies of the System Security Plan and subsequent changes to the plan must be distributed to relevant stakeholders.

4.3 Sul Ross State University must review and update System Security Plans on a recurring basis. This review must occur at an institution-defined frequency or when changes to the Information System or System Security Plan require it.

4.4 System Security Plans must be protected from unauthorized disclosure and modification.

5. Rules of Behavior

Authority - DIR CC: PL-4

5.1 Sul Ross State University must:

5.1.1 Establish and make available to users an acceptable use policy for institutional information resources;

5.1.2 Periodically update the institutional acceptable use policy; and

5.1.3 Require its institutional users to acknowledge the acceptable use policy before authorizing access to information resources.

6. Data Classification, Security, And Retention Requirements for Information Resources Technology Projects

Authority – §TGC 2054.161

6.1.1 On initiation of an information resources technology project, including an application development project and any information resources projects described in subchapter G of Texas Government Code §2054, Sul Ross State University shall classify the data produced from or used in

the project and determine appropriate data security and applicable retention requirements under Texas Government Code §441.185 for each classification.

7. Content of Rules of Behavior

Authority – TSUS Board of Regents

7.1 Sul Ross State University's rules of behavior must address, at minimum, the guidelines established in this section.

7.2 Institutional vs. Individual Purpose

7.2.1 Users accessing institutional information resources are responsible for ensuring that their use of these resources is primarily for institutional purposes and institution-related activities.

7.2.2 Access to information resources carries with it the responsibility for maintaining the security of the institution's information resources.

7.2.3 Rules for incidental use of institutional information resources.

7.2.4 Individuals with authorized access to information resources must ensure that their access permissions are not accessible to or usable by any other individuals.

7.3 Personal vs. Official Representation

7.3.1 Students, faculty, and staff using information resources to reflect the ideas, comments, and opinions of individual members of the Sul Ross State University community must be distinguished from those that represent the official positions, programs, and activities of Sul Ross State University.

7.3.2 Students, faculty, and staff using information resources for purposes of exchanging, publishing, or circulating official institutional documents must follow institutional requirements concerning appropriate content and style.

7.3.3 Sul Ross State University is not responsible for the personal ideas, comments, and opinions of individual members of the Sul Ross State University community expressed through the use of institutional information resources.

7.4 Limitations on the Availability of Information Resources

7.4.1 Sul Ross State University's information resources are finite by nature. All members of the Sul Ross State University community must recognize that certain uses of institutional information resources may be limited or regulated as required to fulfill the institution'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 systems.

7.5 Privacy and Confidentiality of Electronic Documents

7.5.1 No information system can absolutely guarantee the privacy or confidentiality of electronic documents.

7.5.2 Information resources provided by Sul Ross State University are essentially owned by the State of Texas and subject to state oversight. Consequently, persons have no right to privacy in their use of institutional information resources even when using a personal or third-party device to access such resources.

7.5.3 Sul Ross State University should take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons using institutional information resources that Sul Ross State University will not seek access to their electronic messages or documents without their prior consent except where necessary to:

7.5.3.1 Satisfy the requirements of the Texas Public Information Act, or other statutes, laws, or regulations;

7.5.3.2 Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;

7.5.3.3 Protect the integrity of the institution's information resources, and the rights and other property of the institution;

7.5.3.4 Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations; or

7.5.3.5 Protect the rights of individuals working in collaborative situations where information and files are shared.

7.5.4 Sul Ross State University should establish procedures for appropriately preserving the privacy of electronic documents and for determining the methodology by which non-consensual access to electronic documents will be pursued by the institution.

7.6 Failure to Comply with Information Technology Policies

7.6.1 Failure to adhere to the provisions of the IT policies of Sul Ross State University may result in:

7.6.1.1 Suspension or loss of access to institutional information resources;

7.6.1.2 Appropriate disciplinary action under existing procedures applicable to institutional users; and

7.6.1.3 Civil or criminal prosecution

7.6.2 To preserve and protect the integrity of information resources, there may be circumstances where Sul Ross State University must immediately suspend or deny access to the resources. Should an individual's access be suspended under these circumstances, Sul Ross State University shall strive to inform the individual in a timely manner and afford the individual an opportunity to respond. Sul Ross State University shall then determine what disciplinary action is warranted and shall follow the procedures established for such cases.