SRSU Policy: Risk Assessment Policy
SRSU Policy ID: APM 7.36
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 risk assessment.

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 Risk assessment controls 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. Risk Assessment Policy

Authority - DIR Controls Catalog (CC): RA-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

3.1.2 Review and update risk assessment procedures at an institution-defined frequency.

4. Security Categorization

Authority - DIR CC: RA-2, TAC 202.75

4.1 Sul Ross State University's ISO must establish requirements for security categorization of information systems.

4.2 Sul Ross State University must:

4.2.1 Categorize information and information systems, at a minimum of "high", "moderate", or "low", and in accordance with applicable laws, regulations and policies;

4.2.2 Document the security categorization results, including supporting rationale, in the information system security plan; and

4.2.3 Ensure that the security categorization decision is reviewed and approved by information system owner.

5. Risk Assessment

Authority - DIR CC: RA-3, TAC 202

5.1 Sul Ross State University must:

5.1.1 Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

5.1.2 Review and document risk assessment results in a report on a recurring frequency determined by Sul Ross State University's ISO;

5.1.3 Disseminate risk assessment results to the Sul Ross State University ISO;

5.1.4 Perform risk assessments on information systems on a recurring frequency determined by Sul Ross State University or when significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system occur; and

5.2 Authorization of security risk acceptance, transference, or mitigation decisions shall be the responsibility of:

5.2.1 The ISO or their designee(s), in coordination with the information owner, for systems identified with low or moderate residual risk; or

5.2.2 Sul Ross State University's President for all systems identified with a residual high risk.

6. Vulnerability Scanning

Authority - DIR CC: RA-5

6.1 Sul Ross State University must:

6.1.1 Scan for vulnerabilities in each information system and its hosted applications on a recurring frequency, at least annually, in accordance with Sul Ross State University’s established process and when new vulnerabilities potentially affecting systems or applications are identified and reported;

6.1.2 Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards defined by Sul Ross State University’s ISO for:

6.1.2.1 Enumerating platforms, software flaws, and improper configurations;

6.1.2.2 Formatting checklists and test procedures; and

6.1.2.3 Measuring vulnerability impact;

6.1.3 Analyze vulnerability scan reports and results from security control assessments;

6.1.4 Remediate legitimate vulnerabilities in accordance with an organizational assessment of risk; and

6.1.5 Share information obtained from the vulnerability scanning process and security control assessments with appropriate information system custodians in accordance with Sul Ross State University’s internal dissemination procedures.