SRSU Policy: Security Assessment and Authorization Policy
SRSU Policy ID: APM 7.24
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 assessment and authorization.

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 assessment and authorization 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. Security Assessment and Authorization Policy
Authority - DIR Controls Catalog (CC): CA-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Security Assessment and Authorization policy and associated assessment and authorization controls; and

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

4. Security Assessments
Authority - DIR CC: CA-2

4.1 Sul Ross State University must:

4.1.1 Develop a security assessment plan that describes the scope of the assessment including:

4.1.1.1 Security controls and control enhancements under assessment;

4.1.1.2 Assessment procedures to be used to determine security control effectiveness; and

4.1.1.3 Assessment environment, assessment team, and assessment roles and responsibilities;

4.1.2 Assess the security controls in the information system and its environment of operation on a recurring frequency established by the institution's ISO to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

4.1.3 Produce a security assessment report that documents the results of the assessment; and

4.1.4 Provide the results of the security control assessment to appropriate personnel including information owners and custodians.

5. System Interconnections
Authority - DIR CC: CA-3

5.1 Sul Ross State University must:

5.1.1 Through relevant information system owners, authorize interconnections between institutional information systems and other information systems, including those external to the institution;

5.1.2 Use a formalized Interconnection Security Agreement to document interconnections. At minimum, Interconnection Security Agreements must include the following information:

5.1.2.1 Interface characteristics;

5.1.2.2 Security requirements; and

5.1.2.3 The nature of the information communicated.

5.1.3 Regularly review and update as necessary established Interconnection Security Agreements at the time of periodic risk assessments or at an institution-defined frequency.

6. Plan of Action and Milestones

Authority - DIR CC: CA-5

6.1 Sul Ross State University must:

6.1.1 Develop a Plan of Action and Milestones for each information system to document the institution's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls relevant to an information system and to reduce or eliminate known vulnerabilities in the assessed system; and

6.1.2 Update existing plans of action and milestones at an institution-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

7. Security Authorization

Authority - DIR CC: CA-6

7.1 Sul Ross State University must:

7.1.1 Assign a senior-level executive or manager as the Authorizing Official for each information system;

7.1.2 Ensure that the Authorizing Official for an information system authorizes the information system for processing before commencing operations; and

7.1.3 Update the security authorization at the time of periodic risk assessment for the information system or at an institution-defined frequency.

8. Continuous Monitoring

Authority - DIR CC: CA-7

8.1 Sul Ross State University must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

8.1.1 Establishment of metrics to be monitored;

8.1.2 Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;

8.1.3 Ongoing security control assessments in accordance with the institutional continuous monitoring strategy;

8.1.4 Ongoing security status monitoring of institution-defined metrics in accordance with the institutional continuous monitoring strategy;

8.1.5 Correlation and analysis of security-related information generated by assessments and monitoring;

8.1.6 Response actions to address results of the analysis of security-related information; and

8.1.7 Reporting the security status of the institution and the information system to appropriate stakeholders on institutionally defined frequency.

9. Internal System Connections

Authority - DIR CC: CA-9

9.1 Sul Ross State University must:

9.1.1 Authorize internal connections of institution-defined information system components or classes of components to each information system; and

9.1.2 Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.