SRSU Policy: System and Services Acquisition Policy
SRSU Policy ID: APM 7.37
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 system and services acquisition.

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 System and services acquisition 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. System and Services Acquisition Policy

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

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the System and Services Acquisition policy and associated system and services acquisition controls; and

3.1.2 Review and update system and services acquisition procedures at an institution-defined frequency.

4. Allocation of Resources

Authority - DIR CC: SA-2

5. Sul Ross State University must:

5.1 Determine information security requirements for each information system or information system service in mission/business process planning;

5.2 Determine, document, and allocate the resources required to protect each information system or information system service as part of its capital planning and investment control process; and

5.3 Establish a discrete line item for information security in institutional programming and budgeting documentation.

6. System Development Life Cycle

Authority - DIR CC: SA-3

6.1 Sul Ross State University must:

6.1.1 Manage the information system using an institution-defined system development life cycle that incorporates information security considerations;

6.1.2 Define and document information security roles and responsibilities throughout the system development life cycle;

6.1.3 Identify individuals having information security roles and responsibilities; and

6.1.4 Integrate the institutional information security risk management process into system development life cycle activities.

7. Acquisition Process

Authority - DIR CC: SA-4

7.1 Sul Ross State University must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for each information system, system component, or information system service in accordance with applicable federal/state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and institutional mission/business needs:

7.1.1 Security functional requirements;

7.1.2 Security strength requirements;

7.1.3 Security assurance requirements;

7.1.4 Security-related documentation requirements;

7.1.5 Requirements for protecting security-related documentation;

7.1.6 Description of the information system development environment and environment in which the system is intended to operate; and

7.1.7 Acceptance criteria.

8. Information System Documentation

Authority - DIR CC: SA-5

8.1 Sul Ross State University must:

8.1.1 Obtain administrator documentation for each information system, system component, or information system service that describes:

8.1.1.1 Secure configuration, installation, and operation of the system, component, or service;

8.1.1.2 Effective use and maintenance of security functions/mechanisms; and

8.1.1.3 Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

8.1.2 Obtain user documentation for each information system, system component, or information system service that describes:

8.1.2.1 User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

8.1.2.2 Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

8.1.2.3 User responsibilities in maintaining the security of the system, component, or service;

8.1.3 Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and take institution-defined actions in response;

8.1.4 Protect documentation as required, in accordance with the risk management strategy; and

8.1.5 Distribute documentation to institution-defined personnel.

9. External Information System Services

Authority - DIR CC: SA-9

9.1 Sul Ross State University must:

9.1.1 Require that providers of external information system services comply with institutional information security requirements and employ institution-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

9.1.2 Define and document government oversight and user roles and responsibilities with regard to external information system services; and

9.1.3 Employ institution-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

10. Developer Configuration Management

Authority - DIR CC: SA-10

10.1 Sul Ross State University must require the developer of each information system, system component, or information system service to:

10.1.1 Perform configuration management during system, component, or service during at least one of the following stages: design, development, implementation, operation;

10.1.2 Document, manage, and control the integrity of changes to institution-defined configuration items under configuration management;

10.1.3 Implement only institution-approved changes to the system, component, or service;

10.1.4 Document approved changes to the system, component, or service and the potential security impacts of such changes; and

10.1.5 Track security flaws and flaw resolution within the system, component, or service and report findings to institution-defined personnel.