SRSU Policy: System and Communications Policy
SRSU Policy ID: APM 7.38
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 communications protection.

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 communications protection 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 Communications Protection Policy
Authority - DIR Controls Catalog (CC): SC-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the System and Communications Protection policy and associated system and communications protection controls; and

3.1.2 Review and update system and communications protection procedures at an institution-defined frequency.

4. Denial of Service Protection
Authority - DIR CC: SC-5

4.1 Sul Ross State University must protect information systems against or limit the effects of institutionally identified denial of service attacks by employing institutionally defined safeguards.

5. Boundary Protection
Authority - DIR CC: SC-7

5.1 Sul Ross State University must:

5.1.1 Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; and

5.1.2 Implement subnetworks for publicly accessible system components that are either physically or logically separated from internal organizational networks; and

5.1.3 Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

6. Transmission Confidentiality and Integrity
Authority - DIR CC: SC-8

6.1 Each information system must protect the confidentiality and/or integrity of transmitted information.

7. Cryptographic Key Establishment and Management
Authority - DIR CC: SC-12

7.1 Sul Ross State University must establish and manage cryptographic keys for required cryptography employed within each information system in accordance with institutionally defined requirements for key generation, distribution, storage, access, and destruction.

8. Cryptographic Protection
Authority - DIR CC: SC-13

8.1 Each information system must implement institutionally defined cryptographic uses and type of cryptography required for each use in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

9. Collaborative Computing Devices
Authority - DIR CC: SC-15

9.1 Sul Ross State University must:

9.1.1 Prohibit remote activation of collaborative computing devices except for devices specifically defined by the institution; and

9.1.2 Provide an explicit indication of use to users physically present at the devices.

10. Secure Name / Address Resolution Service (Authoritative Source)
Authority - DIR CC: SC-20

10.1 Each information system that provides name resolution services must:

10.1.1 Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

10.1.2 Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

11. Secure Name / Address Resolution Service (Recursive or Caching Resolver)
Authority - DIR CC: SC-21

11.1 Each information system that provides recursive name resolution or name caching must request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

12. Architecture and Provisioning for Name / Address Resolution Service
Authority - DIR CC: SC-22

12.1 Each information system that collectively provides name/address resolution service for Sul Ross State University are fault-tolerant and implement internal/external role separation.

13. Process Isolation
Authority - DIR CC: SC-39

13.1 Each information system must maintain a separate execution domain for each executing process.