SRSU Policy: Network Management Policy
SRSU Policy ID: APM 7.31
Policy Reviewed by: Office of Information Technology
Approval Authority: Executive Cabinet
Approval Date: May 14, 2024
Next Review Date: May 14, 2029

Purpose: The institutional network is a state information resource that exists to achieve the mission, goals, and objectives of Texas State University System and each component institution. Utilization of the network must be consistent with and in support of institutional initiatives. TAC 202 stipulates that access to state information resources must be appropriately managed.

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 Network Management controls by Sul Ross State University must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1.2 Sul Ross State University must ensure the confidentiality, integrity, and availability of its data, voice, and video networks to fulfill its institutional missions and to assure compliance with the management and security standards for public institutions of higher education described in TAC 202.

2. Definitions

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

3. **Network Management Policy**
Authority - TSUS Board of Regents

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Network Management policy and associated network management controls; and

3.1.2 Review and update network management procedures at an institution-defined frequency.

4. Roles and Responsibilities

Authority - TSUS Board of Regents

4.1 Sul Ross State University must:

4.1.1 Define a management framework which clearly delineates the roles and responsibilities for management of the institutional network;

4.1.2 Ensure the administration of the Sul Ross State University network by the Information Resource Manager (IRM) or designee.

4.1.3 Ensure users and administrators of network-connected devices understand their accountability for device management and network usage practices that might result in damage or harm to network operations, performance, or other network-connected devices.

5. Network Address and Device Management

Authority - TSUS Board of Regents

5.1 Sul Ross State University must ensure:

5.1.1 The planning and coordination for the orderly assignment of network addresses; and

5.1.2 The planning and coordination for the correct configuration of devices attached to the network.

5.2 Sul Ross State University must ensure that all devices acting in the role of network infrastructure:

5.2.1 Have a designated device administrator; and

5.2.2 Are registered in a network device registry administered by the Information Resource Manager (IRM) or designee.

5.3 Sul Ross State University must ensure that all devices acting in the role of a server (regardless of their specific function, hardware, software, or location):

5.3.1 Have a designated device administrator; and

5.3.2 Are registered in a network device registry administered by the Information Resource Manager (IRM) or designee.

6. Threat and Incident Response

Authority – TSUS Board of Regents

6.1 Sul Ross State University must ensure:

6.1.1 Network devices or addresses that pose an immediate threat to network operations, performance, or other network-connected devices are disconnected or quarantined to minimize risk until the threat is permanently removed; and

6.1.2 Incident response actions comply with established, policy-defined controls and best practices regarding the preservation and treatment of forensic data.