SRSU Policy: Server Management Policy
SRSU Policy ID: APM 7.39
Policy Reviewed by: Office of Information Technology
Approval Authority: Executive Cabinet
Approval Date: May 14, 2024
Next Review Date: May 14, 2029

Purpose: Institutional servers are state information resource that exist to achieve the mission, goals, and objectives of Sul Ross State University. Utilization of these servers 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 Server Management controls by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1.2 The Texas State University System and its component institutions must ensure the confidentiality, integrity, and availability of their server hardware and software to fulfill their 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 Texas State University System defines technical policy terms in the information technology glossary.

3. Server Management Policy

Authority - TSUS Board of Regents

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Server Management policy and associated server management controls; and

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

4. Roles and Responsibilities

Authority - TSUS Board of Regents

4.1 Sul Ross State University must define a management framework which clearly delineates the roles and responsibilities for management of servers.

4.2 The framework must delineate distinct roles for a server owner and a server administrator that:

4.2.1 Establish the responsibilities of server owners to include:

4.2.1.1 Establishment of server usage requirements;

4.2.1.2 Specification of server access controls (both physical and electronic);

4.2.1.3 Assurance of compliance with state and institutional server management standards; and

4.2.1.4 Designation of a separate primary and secondary server administrator.

4.2.2 Establish the responsibilities of server administrators to include:

4.2.2.1 Enforcement of the owner's usage requirements;

4.2.2.2 Implementation of the owner-specified access controls; and

4.2.2.3 Configuration of the server according to the required standards.

5. Server Management Standards

Authority - TSUS Board of Regents

5.1 Sul Ross State University must:

5.1.1 Develop, document, and make available a server management standard in alignment with established, policy-defined controls, and best practices;

5.1.2 Develop, document, make available, and implement compliance review procedures; and

5.1.3 Ensure that all exceptions to this requirement are documented and justified through risk management decisions.

6. Threat and Incident Response

Authority - TSUS Board of Regents

6.1 Sul Ross State University must ensure:

6.1.1 Servers 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.