SUL ROSS STATE UNIVERSITY

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM™

SRSU Policy: Server Management
SRSU Policy ID: APM 7.08
Policy Reviewed by: Chief Information Officer
Approval Authority: Executive Cabinet
Approval Date: 4/4/2017
Next Review Date: 4/4/2022

Purpose/Reason

Sul Ross State University (SRSU) considers information technology to be a critical enabler in meeting its mission and has made significant investments in information technology assets and capabilities. SRSU recognizes the inherent value of these information technology resources to the state, the Texas State University System, and their constituents. Likewise, Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202) underlines the importance of information technology resources residing in Texas public higher education institutions by requiring state institutions "to protect these assets against unauthorized access, disclosure, modification or destruction," and "to assure the availability, integrity, utility, authenticity, and confidentiality of information." Compliance with this policy contributes to the availability, protection, and appropriate use of the information technology resources of Sul Ross State University.

Policy Statement

It is the policy of Sul Ross State University to ensure the highest level of availability, reliability, confidentiality, and integrity of its servers in fulfillment of our institutional mission.

Policy Specifics

1. Server Purpose and Function

SRSU servers are a state information resource that exists to achieve the mission, goals, and objectives of the university. The purpose and function of any server connected to the SRSU network must also be consistent with and in support of university initiatives, and must adhere to and support the SRSU Risk Management Program. The Sul Ross State University servers are centrally administered by OIT and all servers are required to be registered as an officially sanctioned and managed device in a manner designated by the OIT Device Registration Procedure documented in the OIT Standard Operating Procedures Manual.

2. Server Management Roles and Responsibilities

Distinct roles have been defined for server owners and server administrators, where appropriate. Owners are typically responsible for establishing server usage policies, specifying server access controls (both physical and electronic), and assuring compliance with state and institutional server management standards. Administrators are typically responsible for enforcing the owner's usage policies, implementing the owner-specified access controls, and configuring the server according to the required standards.

3. Conformance with Server Management Best Practices

SRSU owners and administrators work closely as a team to address the following topics: 1

A. Licensing, support, and update management for the operating system and all hosted services and applications
B. Automated threat mitigation (e.g., anti-virus software, host-based firewall, etc.)
C. Protection of any sensitive and confidential data accessible via the server
D. Disablement of prohibited, unauthorized, and unnecessary services
E. Disablement and/or modification of default and unnecessary accounts and passwords
F. Physical and electronic access controls that support role-based access, appropriate separation of duties, and the principle of "least privilege"
G. Backup and recovery
H. User authentication
I. Activity and event logging
J. Network connection requirements and standards (e.g., server registration)

4. Threat and Incident Response

Servers that pose an immediate threat to network operations, performance, or other network connected devices will be disconnected or quarantined to minimize risk until the threat is removed. Incident response best practices are followed to ensure appropriate preservation and treatment of forensic data.

Scope and Applicability

This policy guideline applies to all persons and organizations that manage or utilize information technology resources belonging to Sul Ross State University.

Definitions

Information Technology Resources – any of the following that re owned or supplied by SRSU: usernames or computer accounts, hardware, software, communication networks and devices connected thereto, electronic storage media, related documentation in all forms. Also included are data files resident on hardware or media owned or supplied by SRSU, regardless of their size, source, author, or type of recording media including email message, system logs, web pages and software.

Server – A network device that performs a set of specific services or functions on behalf of other network devices or users.

Server Administrator – The individual designated by the server owner as responsible for performing server management functions.

Server Management – Functions associated with the oversight of server operations. These include controlling user access, establishing/maintaining security measures, monitoring server configuration and performance, and risk assessment and mitigation.

Server Owner – The department head charged with overall responsibility for the server asset in the university's inventory records. The server owner must designate an individual to serve as the primary system administrator and may designate a backup system administrator.

Authority and Responsibility

Questions related to this server management policy should be addressed to the Chief Information Officer or a member of the SRSU Executive Committee.