SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Network Management
SRSU Policy ID: APM 7.05
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. Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202) emphasizes 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 ensure the availability, integrity, utility, authenticity, and confidentiality of information." TAC 202 also stipulates that "access to state information resources must be appropriately managed." Compliance with this policy guideline contributes to the availability, protection, management and appropriate use of the data, voice, and video networks 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 data, voice, and video networks to support and fulfill our institutional missions.

Policy Specifics

Network connections and IP address space management

- The Sul Ross State University institutional network is centrally administered OIT.
- Individuals, grant offices, academic departments or administrative departments at SRSU may not create or support an Internet domain hosted from the University's network without prior approval of the Executive Committee or designee.
- The SRSU OIT network and security administrator(s) will administer the Sul Ross State University IP address space, all network protocols, and the sulross.edu domain and any additional domains approved by the Executive Committee.
- Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to computers.
- The OIT network and security administrator(s) will give prior notice to affected users before making significant changes.
- SRSU departments, faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system to the University network without the prior review and approval of the CIO or designee.
- Physical access to University networking equipment is not permitted without the prior approval of the CIO or designee.

Network firewall and port security

- The University's external Internet firewall policy is to deny all external Internet traffic to the University's network unless explicitly permitted by the CIO or his designee. Access and service restrictions may be enforced by IP address and/or port number. Proxy services may be used in conjunction with the firewall to restrict usage to authenticated individuals.
- The University's internal Internet firewall policy is to deny or limit outbound Internet traffic if rogue behavior is identified or suspected.
- Some network services through standard ports are supported. However, services may be restricted to a limited number of subnets or hosts. For example, SRSU electronic mail may only be sent and received by authorized mail servers on campus. User access to the mail accounts on these servers will be permitted from off-campus through the firewall.
- Most network services through non-standard ports are not supported. Services through non-standard ports may be restricted to a limited number of subnets or hosts. For example, WWW access via the standard HTTP port (Port 80) will be permitted for standard web traffic, but to some other arbitrary port number may not be permitted.
- When appropriate to support the mission of the university, and with approval by OIT, limited encrypted tunnels for access through the firewall to internal resources is permitted using approved VPN software.
- SRSU reserves the right to block or disconnect any computer system or device that allows or is suspected of allowing unauthorized access to the network.

Monitoring and emergency response

- The OIT network and security administrator(s) will monitor traffic logs of the firewall traffic for security auditing purposes based upon retention schedules set by the CIO or designee.
- The CIO or designee reserves the right to monitor, access, retrieve, read and/or disclose data communications as legally appropriate.
- Recognizing the immediacy required to respond to security breaches or published security vulnerabilities, the OIT network and security administrator(s) are authorized to remove any server from operation at anytime for the purpose of installing security patches; updating virus protection software; and/or for securing forensic evidence.

Enforcement and recourse

- The University considers any violation of the Network Management Policy to be a serious offense, and reserves the right to test and monitor security, including copying and examining any files or information resident on university computer systems allegedly related to unacceptable use.
- Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network in any way is subject to immediate disconnection from the University's network. The CIO or designee may require specific security improvements where potential security problems are identified.
- Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. This includes but is not limited to attaching unregistered devices to the network; sharing passwords; leaving systems unattended that are logged into security sensitive servers; unauthorized monitoring of the network; and assisting someone else or requesting someone else to circumvent security or administrative access controls.
- Persons responsible for policy violations are subject to action in accordance with student, faculty and staff disciplinary policies and procedures and possible prosecution from local, state and federal authorities.
- To preserve and protect the integrity of information technology resources, there may be circumstances where SRSU must immediately suspend or deny access to the resources. Should an individual's access be suspended under these circumstances, the institution shall strive to inform the individual in a timely manner

and afford the individual an opportunity to respond. The institution shall then determine what disciplinary action is warranted and shall follow the procedures established for such cases.

Scope and Applicability

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

Authority and Responsibility

Questions related to this policy statement should be addressed to the Chief Information Officer.