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: 2-25-2014
Next Review Date: 2-25-2016

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 the Texas State University System and its component institutions.

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 by the Information Resource Manager.
- Any device acting as a server and administered by the Information Resource Manager or designee must be registered as an officially sanctioned and managed device in a manner designated in OIT’s Device Registration procedures.
- Individuals, grant offices, academic departments or administrative departments at SRSU may not create nor 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 or a member of the SRSU Executive Cabinet.

Additional background, Related Policies, and other References

In addition to the general guidelines set forth in this document, network management policies may be affected by a number of other legal requirements and ethical principles. While it is not possible to list all potentially applicable laws and regulations, the following are particularly likely to have implications for network management policies:

1. The federal Family Educational Rights and Privacy Act (commonly known as FERPA) - restricts access to personally identifiable information from students’ education records.

2. Texas Administrative Code, Title 5, Subtitle A, Chapter 552: The Texas Public Information Act (formerly known as the Texas Open Records Act) – provides that all information collected, assembled, or maintained by governmental bodies is public information and available to the public during normal business hours, unless the information falls within certain exceptions specified in the Act.

3. Texas Administrative Code, Title 1, Part 10, Chapter 202 - Regulations from the Department of Information Resources establishing requirements for State agencies regarding information resources security.

4. Texas Penal Code, Chapter 33: Computer Crimes - Texas law pertaining to computer crimes. This statute specifically prohibits unauthorized access to University computers, unauthorized access to stored data, or dissemination of passwords or other confidential information to facilitate unauthorized access to the University’s computer system or data.

5. Texas Penal Code, § 37.10: Tampering with Governmental Record - Prohibits any alteration, destruction, or false entry of data that impairs the validity, legibility or availability of any record maintained by the University.

6. United States Code, Title 18, § 1030: Fraud and Related Activity in Connection with Computers - Federal law specifically pertaining to computer crimes. Among other stipulations, prohibits unauthorized and fraudulent access to information resources.

7. Computer Fraud and Abuse Act of 1986 (Part of 18 U.S.C. § 1030) - Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.


9. Federal Copyright Law - Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.

10. Digital Millennium Copyright Act - Signed into law on October 20, 1998, as Public Law 105-304. Created to address the digitally networked environment, the DMCA implements the WIPO Internet Treaties; establishes safe harbors for online service providers; permits temporary copies of programs during the
performance of computer maintenance; and makes miscellaneous amendments to the Copyright Act, including amendments that facilitate Internet broadcasting.

11. Electronic Communications Privacy Act of 1986 - Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

12. Computer Software Rental Amendments Act of 1990 - Deals with the unauthorized rental, lease, or lending of copyrighted software.

13. Texas Government Code § 556.004 - Prohibits using state resources or programs to influence elections or to achieve any other political purpose.


Students, faculty and staff 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 technology resources.