SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Physical Access Policy
SRSU Policy ID: APM 7.14
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) has made a significant investment in hardware and software systems. The systems must be kept safe and secure from tampering or accidental damage. Some of the systems contain Confidential and/or Sensitive data. SRSU has the responsibility to document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction (TAC 202.76a).

Policy Statement

Unauthorized personnel are restricted from access to the SRSU data centers and switch closets.

Policy Specifics

SRSU system and network administrators and *some* authorized Physical Plant employees may have physical access to SRSU data centers and switch closets. Third party contractors who *have not* been waived by contracts must be accompanied at all times by the Director of Technical Services or his/her designee of SRSU OIT while in SRSU data centers and switch closets.

All contractors must sign in and out via a form provided in each data center or switch closet the employee enters. The form will require sign-in time and sign-out time. Video surveillance systems may be employed in the data center or switch closet and the employee or contractor should have no expectation of privacy while in those restricted areas.

Scope and Applicability

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