SRSU Policy: Maintenance Policy
SRSU Policy ID: APM 7.29
Policy Reviewed by: Office of Information Technology
Approval Authority: Executive Cabinet
Approval Date: May 14, 2024
Next Review Date: May 14, 2029

Purpose: The purpose of this policy is to define information security controls regarding maintenance.

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 Maintenance controls implemented by Sul Ross State University must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Sul Ross State University defines technical policy terms in the information technology glossary.

3. System Maintenance Policy and Procedures
Authority - DIR Controls Catalog (CC): MA-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the maintenance policy and associated maintenance controls; and

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

4. Controlled Maintenance

Authority - DIR CC: MA-2

4.1 Information system custodians are responsible for scheduling, performing, documenting, and reviewing records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or Sul Ross State University requirements.

4.2 Information system custodians are responsible for approving and monitoring all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

4.3 Sul Ross State University must require that information system owners or custodians explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

4.4 Information system owners and custodians must ensure that equipment is sanitized to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

4.5 Information system owners and custodians must check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

4.6 Information system owners and custodians must update appropriate organizational maintenance records following maintenance or repair actions.

5. Nonlocal Maintenance

Authority - DIR CC: MA-4

5.1 Sul Ross State University must:

5.1.1 Approve and monitor nonlocal maintenance and diagnostic activities;

5.1.2 Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

5.1.3 Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

5.1.4 Maintain records for nonlocal maintenance and diagnostic activities; and

5.1.5 Terminate session and network connections when nonlocal maintenance is completed.

6. Maintenance Personnel

Authority - DIR CC: MA-5

6.1 Sul Ross State University must:

6.1.1 Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

6.1.2 Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations; and

6.1.3 Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.