SRSU Policy: Configuration Management Policy
SRSU Policy ID: APM 7.25
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 around configuration management.

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 Configuration management 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. Configuration Management Policy
Authority - DIR Controls Catalog (CC): CM-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Configuration Management policy and associated configuration management controls; and

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

4. Baseline Configuration
Authority - DIR CC: CM-2

4.1 Sul Ross State University must develop, document, and maintain under configuration control, a current baseline configuration of the information system**.**

5. Security Impact Analysis
Authority - DIR CC: CM- 4

5.1 Sul Ross State University must analyze changes to information systems to determine potential security impacts prior to change implementation.

6. Configuration Settings
Authority - DIR CC: CM- 6

6.1 Sul Ross State University must:

6.1.1 Establish and document configuration settings for information technology products employed within the information system using institution-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

6.1.2 Implement the configuration settings;

6.1.3 Identify, document, and approve any deviations from established configuration settings for institution-defined information system components based on institution-defined operational requirements; and

6.1.4 Monitor and control changes to the configuration settings in accordance with institutional policies and procedures.

7. Least Functionality
Authority - DIR CC: CM- 7

7.1 Sul Ross State University must:

7.1.1 Configure each information system to provide only essential capabilities; and

7.1.2 Prohibit or restrict the use of institution-defined functions, ports, protocols, and/or services.

8. Information System Component Inventory
Authority - DIR CC: CM- 8

8.1 Sul Ross State University must:

8.1.1 Develop and document an inventory of information system components that:

8.1.1.1 Accurately reflects the current information system;

8.1.1.2 Includes all components within the Authorization Boundary of the information system;

8.1.1.3 Is at the level of granularity deemed necessary for tracking and reporting; and

8.1.1.4 Includes institution-defined information deemed necessary to achieve effective information system component accountability; and

8.1.2 Review and update the information system component inventory at an institution-defined frequency.

9. Software Usage Restrictions
Authority - DIR CC: CM- 10

9.1 Sul Ross State University must:

9.1.1 Use software and associated documentation in accordance with contract agreements and copyright laws;

9.1.2 Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

9.1.3 Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. User-Installed Software
Authority - DIR CC: CM- 11

10.1 Sul Ross State University must:

10.1.1 Establish institution-defined policies governing the installation of software by users;

10.1.2 Enforce software installation policies through institution-defined methods; and

10.1.3 Monitor policy compliance at institution-defined frequency.