SRSU Policy: System and Information Integrity Policy
SRSU Policy ID: APM 7.40
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 system and information integrity.

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 System and information 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 and Information Integrity Policy
Authority - DIR Controls Catalog (CC): SI-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the System and Information Integrity policy and associated system and information integrity controls; and

3.1.2 Review and update system and information integrity procedures at an institution-defined frequency.

4. Flaw Remediation
Authority - DIR CC: SI-2

4.1 Sul Ross State University must:

4.1.1 Identify, report, and correct information system flaws;

4.1.2 To the extent practicable, test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

4.1.3 Install security-relevant software and firmware updates within an institution-defined time period of the release of the updates; and

4.1.4 Incorporate flaw remediation into the institutional configuration management process.

5. Malicious Code Protection
Authority - DIR CC: SI-3

5.1 Sul Ross State University must:

5.1.1 Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

5.1.2 Update malicious code protection mechanisms whenever new releases are available in accordance with institutional configuration management policy and procedures;

5.1.3 Configure malicious code protection mechanisms to:

5.1.3.1 Perform periodic scans of the information system at an institution-defined frequency and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with institutional security policy; and

5.1.3.2 Perform one or more of the following in response to malicious code detection: block malicious code; quarantine malicious code; send alert to administrator; or perform another institution-defined action; and

5.1.4 Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

6. Information System Monitoring
Authority - DIR CC: SI-4

6.1 Sul Ross State University must:

6.1.1 Monitor each information system to detect:

6.1.1.1 Attacks and indicators of potential attacks in accordance with institution-defined monitoring objectives; and

6.1.1.2 Unauthorized local, network, and remote connections;

6.1.2 Identify unauthorized use of the information system through institution-defined techniques and methods;

6.1.3 Deploy monitoring devices:

6.1.3.1 Strategically within the information system to collect institutional-determined essential information; and

6.1.3.2 At ad hoc locations within the system to track specific types of transactions of interest to Sul Ross State University;

6.1.4 Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

6.1.5 Heighten the level of information system monitoring activity whenever there is an indication of increased risk to institutional operations and assets, individuals, or other organizations on law enforcement information, intelligence information, or other credible sources of information;

6.1.6 Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

6.1.7 Provide institution-defined information system monitoring information to institution-defined personnel as needed and/or at an institution-defined frequency.

7. Security Alerts, Advisories, and Directives

Authority - DIR CC: SI-5

7.1 Sul Ross State University must:

7.1.1 Receive information system security alerts, advisories, and directives from institution-defined external organizations on an ongoing basis;

7.1.2 Generate internal security alerts, advisories, and directives as deemed necessary;

7.1.3 Disseminates security alerts, advisories, and directives to institution-defined personnel and/or institution-defined external organizations; and

7.1.4 Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

8. Information Handling and Retention

Authority - DIR CC: SI-12

8.1 Sul Ross State University must handle and retain information within each information system and information output from each system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.