SRSU Policy: Audit and Accountability Policy
SRSU Policy ID: APM 7.23
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 audit and accountability.

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 Audit and accountability controls implemented by component institutions 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. Audit and Accountability Policy
Authority - DIR Controls Catalog (DIR CC): AU-1

3.1 Sul Ross State University must:

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

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

4. Audit Events

Authority - DIR CC: AU-2

4.1 Sul Ross State University must determine the capability of an information system for auditing institution-defined events.

4.2 Sul Ross State University ISO, or designee, shall coordinate with information system owners and custodians to help guide the selection of auditable security events.

4.3 Sul Ross State University must provide a rationale for why institution-defined auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

4.4 Sul Ross State University must determine:

4.4.1 What subset of events defined in 4.1 are to be audited within an information system; and,

4.4.2 The frequency at which events will be audited; or

4.4.3 Situations requiring auditing.

5. Content of Audit Records

Authority - DIR CC: AU-3

5.1 Sul Ross State University must ensure that information systems are configured to generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

6. Audit Storage Capacity

Authority - DIR CC: AU-4

6.1 Sul Ross State University must allocate audit record storage capacity in accordance with institution-defined audit record storage requirements.

7. Response to Audit Processing Failures

Authority - DIR CC: AU-5

7.1 Information systems must be configured to alert appropriate information system custodians in the event of an audit processing failure.

8. Audit Review, Analysis, and Reporting

Authority - DIR CC: AU-6

8.1 Sul Ross State University must review and analyze information system audit records and report actionable findings to the appropriate information system custodians.

8.2 Review and analysis of information system audit records must occur at a frequency or in a manner determined by Sul Ross State University.

9. Protection of Audit Information

Authority - DIR CC: AU-9

9.1 Sul Ross State University must ensure that information systems protect audit information and audit tools from unauthorized access, modification, and deletion.

10. Audit Record Retention

Authority - DIR CC: AU-11

10.1 Sul Ross State University must retain audit records for a period no less than is required by its records retention policy and in order to provide sufficient support for after-the-fact investigations of security incidents.

11. Audit Generation

Authority - DIR CC: AU-12

11.1 Sul Ross State University must ensure that information systems:

11.1.1 Provide audit record generation capability for the auditable events defined in 4.1;

11.1.2 Allow information system custodians to select which auditable events are to be audited by specific components of the information system; and

11.1.3 Generate audit records for the events defined in 4.4.1 with the content defined in 5.1.