SRSU Policy: Access Control Policy
SRSU Policy ID: APM 7.21
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 access control.

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 Access controls 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. Access Control Policy
Authority - DIR Controls Catalog (DIR CC): AC-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Access Control policy and associated access controls; and

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

4. Account Management
Authority - DIR CC: AC-2, TAC 202.72

4.1 Sul Ross State University must:

4.1.1 Identify and document, in consultation with the SRSU ISO and IRM, the types of information system accounts that support organizational missions and business functions;

4.1.2 Assign account manager responsibilities for information system accounts to the respective information owner;

4.1.3 Establish conditions for group and role membership;

4.1.4 Require the respective information owner to specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

4.1.5 Require approval from the information owner for requests to create information system accounts;

4.1.6 Require the respective information custodian to create, enable, modify, disable, and remove information system accounts in accordance with institution-defined procedures;

4.1.7 Require the respective information custodian to monitor the use of information system accounts;

4.1.8 Notify account managers:

4.1.8.1 When accounts are no longer required;

4.1.8.2 When users are terminated or transferred; and

4.1.8.3 When individual information system usage or need-to-know changes;

4.1.9 Require that the respective information owner authorize access to the information system based on:

4.1.9.1 A valid access authorization;

4.1.9.2 Intended system usage; and

4.1.9.3 Other attributes as required by Sul Ross State University or associated missions/business functions;

4.1.10 Require respective information custodians to review accounts for compliance with account management requirements at an institution-defined frequency; and

4.1.11 Require respective information owners and information custodians to establish processes for reissuing shared/group account credentials (if deployed) when individuals are removed from a group.

5. Account Enforcement
Authority - DIR CC: AC-3

5.1 Sul Ross State University must ensure that information systems enforce approved authorizations for logical access to information and system resources in accordance with applicable, institution-defined access control policies.

6. Separation of Duties
Authority - DIR CC: AC-5

6.1 Sul Ross State University must:

6.1.1 Ensure that duties of individuals are appropriately separated based on institution-defined criteria;

6.1.2 Document separation of duties of individuals; and

6.1.3 Define information system access authorizations to support separation of duties.

7. Unsuccessful Logon Attempts
Authority - DIR CC: AC-7

7.1 Sul Ross State University must ensure that each information system:

7.1.1 Enforces an institution-defined limit of consecutive, invalid logon attempts by a user during an institution-defined time period; and

7.1.2 Automatically performs one of the following actions when the maximum number of unsuccessful attempts is exceeded:

7.1.2.1 Locks the account or node for an institution-defined time period;

7.1.2.2 Locks the account or node until released by an administrator; or

7.1.2.3 Delays the next logon prompt according to an institution-defined delay algorithm.

8. System Use Notification
Authority - DIR CC: AC-8

8.1 Sul Ross State University must ensure that each information system:

8.1.1 Displays to human users at logon interfaces an institution-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

8.1.1.1 Users are accessing a Sul Ross State University information system;

8.1.1.2 Information system usage may be monitored, recorded, and subject to audit;

8.1.1.3 Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

8.1.1.4 Use of the information system indicates consent to monitoring and recording;

8.1.2 Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

8.1.3 For publicly accessible systems that do not have logon interfaces:

8.1.3.1 Displays system use information under institution-defined conditions before granting further access;

8.1.3.2 Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

8.1.3.3 Includes a description of the authorized uses of the system.

9. Permitted Actions Without Identification or Authentication
Authority - DIR CC: AC-14

9.1 Sul Ross State University must:

9.1.1 Identify and define user actions that can be performed on Sul Ross State University information systems without identification or authentication consistent with institutional missions/business functions; and

9.1.2 Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

10. Remote Access
Authority - DIR CC: AC-17

10.1 Sul Ross State University must:

10.1.1 Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

10.1.2 Authorize remote access to each information system prior to allowing such connections.

11. Wireless Access
Authority - DIR CC: AC-18

11.1 Sul Ross State University must:

11.1.1 Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

11.1.2 Authorizes wireless access to the information system prior to allowing such connections.

12. Access Control for Mobile Devices
Authority - DIR CC: AC-19

12.1 Sul Ross State University must:

12.1.1 Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for institution-controlled mobile devices; and

12.1.2 Authorize the connection of mobile devices to Sul Ross State University information systems.

13. Use of External Information Systems
Authority - DIR CC: AC-20

13.1 Sul Ross State University must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

13.1.1 Access the information system from external information systems; and

13.1.2 Process, store, or transmit institution-controlled information using external information systems.

14. Publicly Accessible Content
Authority- DIR CC: AC-22

14.1 Sul Ross State University must:

14.1.1 Designate individuals authorized to post information onto a publicly accessible information systems;

14.1.2 Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

14.1.3 Review, based on institution-defined criteria, the proposed content of information prior to posting onto publicly accessible information systems to ensure that nonpublic information is not included; and

14.1.4 Review, based on institution-defined criteria, the content on the publicly accessible information system for nonpublic information at institution-defined frequencies and removes such information, if discovered.