SRSU Policy: Identification and Authentication Policy
SRSU Policy ID: APM 7.27
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 identification and authentication.

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 Identification and authentication 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. Identification and Authentication Policy
Authority - DIR Controls Catalog (CC): IA-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Identification and Authentication policy and associated identification and authentication controls; and

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

4. Identification and Authentication

Authority - DIR CC: IA-2

4.1 Sul Ross State University must ensure that information systems uniquely identify and authenticate institutional users (or processes acting on behalf of institutional users).

5. Identifier Management

Authority - DIR CC: IA-4

5.1 Sul Ross State University must manage information system identifiers by:

5.1.1 Receiving authorization from institution-defined personnel to assign an individual, group, role, or device identifier;

5.1.2 Selecting an identifier that identifies an individual, group, role, or device;

5.1.3 Assigning the identifier to the intended individual, group, role, or device;

5.1.4 Preventing reuse of identifiers for an organization-defined time period; and

5.1.5 Disabling the identifier after institution-defined time period of inactivity.

6. Authenticator Management

Authority - DIR CC: IA-5

6.1 Sul Ross State University must manage information system authenticators by:

6.1.1 Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

6.1.2 Establishing initial authenticator content for authenticators defined by the institution;

6.1.3 Ensuring that authenticators have sufficient strength of mechanism for their intended use;

6.1.4 Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

6.1.5 Changing default content of authenticators prior to information system installation;

6.1.6 Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

6.1.7 Changing/refreshing authenticators at an institution-defined time period by authenticator type;

6.1.8 Protecting authenticator content from unauthorized disclosure and modification;

6.1.9 Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

6.1.10 Changing authenticators for group/role accounts when membership to those accounts changes.

7. Authenticator Feedback

Authority - DIR CC: IA-6

7.1 Sul Ross State University must ensure that information systems obscure feedback of authentication information entered during the authentication process.

8. Cryptographic Module Authentication

Authority - DIR CC: IA-7

8.1 Sul Ross State University must follow all applicable laws and regulation regarding the use of cryptographic module authentication mechanisms for information systems.

9. Identification and Authentication (Non-Organizational Users)

Authority - DIR CC: IA-8

9.1 Sul Ross State University must ensure that information systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).