**SRSU Policy: Personnel Security Policy**
**SRSU Policy ID: APM 7.35**
**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 personnel security.

**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 Personnel security 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. Personnel Security Policy
**Authority - DIR Controls Catalog (CC): PS-1**

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Personnel Security policy and associated personnel security controls; and

3.1.2 Review and update personnel security procedures at an institution-defined frequency.

### 4. Position Risk Designation

**Authority - DIR CC: PS-2**

4.1 Sul Ross State University must:

4.1.1 Assign a risk designation to all institutional positions;

4.1.2 Establish screening criteria for individuals filling those positions; and

4.1.3 Review and update position risk designations at an institution-defined frequency.

## 5. Personnel Screening

**Authority - DIR CC: PS-3**

5.1 Sul Ross State University must:

5.1.1 Screen individuals prior to authorizing access to information systems; and

5.1.2 Rescreen individuals when institution-defined conditions require rescreening.

## 6. Personnel Termination

**Authority - DIR CC: PS-4**

6.1 Sul Ross State University, upon termination of an individual's employment, must:

6.1.1 Disable information system access and terminate/revoke any authenticators/credentials associated with the individual within an institution-defined time period;

6.1.2 Conduct exit interviews that include a discussion of institution-defined information security topics that include review of any signed non-disclosure agreements and secure disposition of university data from personal devices in a manner stipulated by the institution;

6.1.3 Retrieve all security-related, institutional information system-related property;

6.1.4 Retain access to institutional information and information systems formerly controlled by terminated individual; and

6.1.5 Notify institution-defined personnel within an institution-defined time period.

## 7. Personnel Transfer

**Authority - DIR CC: PS-5**

7.1 Sul Ross State University must:

7.1.1 Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when

individuals are reassigned or transferred to other positions within the institution;

7.1.2 Initiate transfer or reassignment actions within an institution-defined time period following the formal transfer action;

7.1.3 Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and

7.1.4 Notify institution-defined personnel within an institution-defined time period.

## 8. Access Agreements

**Authority - DIR CC: PS-6**

8.1 Sul Ross State University must:

8.1.1 Develop and document access agreements for institutional information systems;

8.1.2 Review and update the access agreements at an institution-defined frequency; and

8.1.3 Ensure that individuals requiring access to institutional information and information systems:

8.1.3.1 Sign appropriate access agreements prior to being granted access; and

8.1.3.2 Re-sign access agreements to maintain access to institutional information systems when access agreements have been updated or at an institution-defined frequency.

## 9. Third-Party Personnel Security

**Authority - DIR CC: PS-7**

9.1 Sul Ross State University must:

9.1.1 Establish personnel security requirements including security roles and responsibilities for third-party providers;

9.1.2 Require third-party providers to comply with personnel security policies and procedures established by Sul Ross State University;

9.1.3 Document personnel security requirements;

9.1.4 Require third-party providers to notify institution-defined personnel of any personnel transfers or terminations of third-party personnel who possess institutional credentials and/or badges, or who have information system privileges within an institution-defined time period; and

9.1.5 Monitors provider compliance.

## 10. Personnel Sanctions

**Authority - DIR CC: PS-8**

10.1 Sul Ross State University must:

10.1.1 Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

10.1.2 Notify institution-defined personnel within institution-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.