SRSU Policy: Incident Response Policy
SRSU Policy ID: APM 7.28
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 incident response.

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 Incident response 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. Incident Response Policy
Authority - DIR Controls Catalog (CC): IR-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Incident Response policy and associated incident response controls; and

3.1.2 Review and update incident response procedures at an institution-defined frequency.

4. Incident Response Training

Authority - DIR CC: IR-2

4.1 Sul Ross State University must provide incident response training to information system users consistent with their assigned roles and responsibilities:

4.1.1 Within an institution-defined time period of assuming an incident response role or responsibility;

4.1.2 When required by information system changes; and

4.1.3 At an institution-defined frequency thereafter.

5. Incident Handling

Authority - Texas Administrative Code (TAC): 202.73(b); DIR CC: IR-4

5.1 Sul Ross State University must:

5.1.1 Implement and maintain an incident handling capability to include preparation, detection and analysis, containment, eradication, recovery and coordination of incident handling activities with contingency planning activities;

5.1.2 Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

5.1.3 Assess the significance of information security incidents based on the business impact on the affected resources and the current potential technical effect of the incident.

6. Incident Monitoring

Authority - TAC 202.73; DIR CC: IR-5

6.1 Sul Ross State University must track and document information system security incidents.

7. Incident Reporting

Authority - TAC 202.73; DIR CC: IR-6

7.1 Sul Ross State University must:

7.1.1 Require personnel to report suspected security incidents to the Sul Ross State University's Information Security Officer (ISO) or authorized designee using institution-defined procedures;

7.1.2 Develop policies and mechanisms providing for notification to the designated ISO of any Suspected Data Breach within 48 hours of discovery;

7.1.3 Promptly report security incidents to the Department of Information Resources (DIR) when the security incident is assessed to:

7.1.3.1 Propagate to other state Information Systems;

7.1.3.2 Result in criminal violations that shall be reported to law enforcement in accordance with state or federal information security or privacy laws; or

7.1.3.3 Involve the unauthorized disclosure or modification of confidential information.

7.1.4 Report summary security incident information monthly to DIR no later than 9 calendar days after the end of the month; and

7.1.5 Establish reporting procedures which include a requirement that all personnel report suspected incidents to the ISO within a timeframe and method determined by the institution.

7.2 If an information security incident is required to be reported to the DIR under Texas Government Code Sec. 2054.1125 or the "Urgent Incident Report" rules per Texas Administrative Code 202.73(b), the established event reporting and escalation procedures shall also require notification to the Texas State University System Administration via the Vice Chancellor and Chief Financial Officer and the Chief Audit Executive in a similar reporting manner and timeline.

8. Incident Response Assistance

Authority - DIR CC: IR-7

8.1 As an element of incident response capabilities, Sul Ross State University must provide incident response resources that advise and assist users of information resources in handling and reporting security incidents.

8.2 Incident response resources are determined by Sul Ross State University's Information Security Officer and may be comprised of technical support personnel, verified third-party consultants, and other resources.

9. Incident Response Plan

Authority - DIR CC: IR-8

9.1 Sul Ross State University must:

9.1.1 Develop an incident response plan that:

9.1.1.1 Provides the institution with a roadmap for implementing its incident response capability;

9.1.1.2 Describes the structure and organization of the incident response capability;

9.1.1.3 Provides a high-level approach for how the incident response capability fits in to the overall institution;

9.1.1.4 Meets the unique requirements of the institution, which relate to mission, size, structure, and functions;

9.1.1.5 Defines reportable incidents;

9.1.1.6 Provides metrics for measuring the incident response capability within the institution;

9.1.1.7 Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

9.1.1.8 Is reviewed and approved by appropriate, institution-defined leadership.

9.1.2 Distribute copies of the incident response plan to appropriate personnel in an institution-defined manner;

9.1.3 Review and update the incident response plan as changes or problems are encountered or at least once annually, whichever occurs first;

9.1.4 Communicate changes to the incident response plan to appropriate personnel in an institution-defined manner; and

9.1.5 Protect the incident response plan from unauthorized disclosure and modification.