SRSU Policy: Contingency Planning Policy
SRSU Policy ID: APM 7.26
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 contingency planning.

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 Contingency planning 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. Contingency Planning Policy
Authority -DIR Controls Catalog (CC): CP-1

3.1 Sul Ross State University must:

3.1.1 Develop procedures to facilitate the implementation of the Contingency Planning policy and associated contingency planning controls; and

3.1.2 Review and update contingency planning procedures at an institution-defined frequency.

4. Contingency Plan

Authority - DIR CC: CP-2

4.1 Sul Ross State University must:

4.1.1 Develop a contingency plan for each information system that:

4.1.1.1 Identifies essential missions and business functions and associated contingency requirements;

4.1.1.2 Provides recovery objectives, restoration priorities, and metrics;

4.1.1.3 Addresses contingency roles, responsibilities, and assigned individuals with contact information;

4.1.1.4 Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

4.1.1.5 Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

4.1.1.6 Is reviewed and approved by institution-defined personnel or roles;

4.1.2 Distribute copies of the contingency plan to institution-defined key contingency personnel (identified by name and/or by role) and institutional elements;

4.1.3 Coordinate contingency planning activities with incident handling activities;

4.1.4 Review the contingency plan for the information system at an institution-defined frequency;

4.1.5 Update the contingency plan to address changes to the institution, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

4.1.6 Communicate contingency plan changes to institution-defined key contingency personnel (identified by name and/or by role) and institutional elements; and

4.1.7 Protect the contingency plan from unauthorized disclosure and modification.

5. Contingency Training

Authority - DIR CC: CP-3

5.1 Sul Ross State University must provide contingency training to information system users consistent with assigned roles and responsibilities:

5.1.1 Within an institution-defined time period of assuming a contingency role or responsibility;

5.1.2 When required by information system changes; and

5.1.3 On an institution-defined frequency thereafter.

6. Contingency Testing
Authority - DIR CC: CP-4

6.1 Sul Ross State University must:

6.1.1 Test the contingency plan for the information system on an institution-defined frequency using institution-defined tests to determine the effectiveness of the plan and the institutional readiness to execute the plan;

6.1.2 Review the contingency plan test results; and

6.1.3 Initiate corrective actions, if needed.

7. Alternate Storage Site
Authority - DIR CC: CP-6

7.1 Sul Ross State University must:

7.1.1 Establish an alternate storage site for Mission Critical information systems including necessary agreements to permit the storage and retrieval of information system backup information; and

7.1.2 Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

8. Information System Backup
Authority - DIR CC: CP-9

8.1 Sul Ross State University must:

8.1.1 Conduct backups of user-level information contained in the information system consistent with recovery time and recovery point objectives;

8.1.2 Conduct backups of system-level information contained in the information system consistent with recovery time and recovery point objectives;

8.1.3 Conduct backups of information system documentation including security-related documentation consistent with recovery time and recovery point objectives; and

8.1.4 Protect the confidentiality, integrity, and availability of backup information at storage locations.

9. Information System Recovery and Reconstitution

Authority - DIR CC: CP-10

9.1 Sul Ross State University must have the capability for recovery and reconstitution of each information system to a known state after a disruption, compromise, or failure.