Contingency Plan Policy

Purpose:
The purpose is to establish and implement, as needed, policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain sensitive information.

A contingency plan is a routinely updated plan for responding to a system emergency that includes performing backups, preparing critical facilities, and appropriately detailed migration plans that can be used to facilitate continuity of operations in the event of an emergency and recovering from a disaster.

Scope:
This policy applies to Sweetwater County School District #1 in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Policy:
Sweetwater County School District #1 will develop contingency plan documents to identify core activities in the areas of Data Backup Plan, Disaster Recovery Plan, Emergency Mode Operation Plan, Testing and Revision, and Applications and Data Criticality Analysis.

Sweetwater County School District #1 will develop and implement a contingency plan to ensure the confidentiality, integrity, and availability of sensitive information during and after an emergency.

The core objectives of contingency planning include the capability to:

- Restore operations at an alternate site (if necessary)
- Recover operations using alternate equipment (if necessary)
- Perform some or all of the affected business processes using other means

The contingency plan must address Information Technology (IT) system components such as:

- Local, wide area and wireless networks including Internet access (if critical to the operation of the business)
- Server systems such as file, application, print and database
- Websites
- Security systems such as firewalls, authentication servers, and intrusion detection
- Desktop, laptop, mobile devices

Sweetwater County School District #1 will follow the recommendations of The National Institute of Standards and Technology (NIST) in the area of contingency planning.

Responsibilities:
The Security Officer is responsible for implementation of the Contingency Plan Policy.

Compliance:
District and/or legal action may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s):
Procedures related to the Contingency Plan include:

- Data backup

- Disaster recovery
- Emergency mode operations
- Testing and revision
- Applications and data criticality analysis

Form(s):

- Business Impact Analysis (BIA) Report

References:

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- International Standards Organization (ISO 27002).
- National Institute of Standards and Technology (NIST)

Adopted: 04/09/18