



**SWEETWATER COUNTY
SCHOOL DISTRICT #1**

Agenda Item 11-a

Recommendation for the approval of the Contingency Plan Policy

Contingency Plan Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

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 will be developed for the entire enterprise.~~ 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. ~~The NIST recommends following seven key steps to address the requirements of contingency planning. These seven key steps for contingency planning are:~~

1. Develop the contingency policy objective statement
2. Conduct a Business Impact Analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Create the contingency plan
6. Conduct testing and training
7. Review and maintenance

Let us review of the steps to better understand how we may be able to meet contingency planning requirements.

Step 1: Contingency Policy Objective Statement

The first step for the organization to address the requirements associated with contingency planning is to very clearly define the contingency planning policy. The core objective of the policy statement is to establish the organizational framework and responsibilities for contingency planning. NIST recommends that the contingency policy address the following topics:

- Roles and responsibilities
- Scope of policy with respect to systems/platforms and organizations functions subject to contingency planning
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Frequency of backups and storage of backup media

Step 2: Business Impact Analysis (BIA)

One of the critical steps in contingency planning is Business Impact Analysis (BIA). BIA helps to identify and prioritize critical Information Technology (IT) systems and components. IT systems may have numerous components, interfaces and processes. BIA enables a complete characterization of:

- System requirements
- Processes
- Interdependencies

As part of the BIA process, information is collected, analyzed and interpreted. The information provides the basis for defining contingency requirements and priorities.

The objective is to understand the impact of a threat on the business. The impact of the threat may be economical, operational or both. Questionnaires or survey tools may be used to collect the information.

BIA is performed at the beginning of disaster recovery and continuity planning to specifically identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. A key objective is to identify all critical systems that are required for the continuity of the business. Further, a determination of the time it would take to recover such systems in the event of a loss.

The critical steps for BIA include the need to:

1. Identify critical business functions
2. Identify disruption impacts and allowable outage times
3. Develop recovery priorities

Step 3: Preventive Controls

The BIA provides vital information regarding system availability and recovery requirements. It may be possible to mitigate some outage impacts identified in the BIA through preventive controls. The objective of preventive controls is to deter, detect, and/or reduce impacts to the system. Wherever possible, preventive controls are preferable to actions to recover the system after a disruption.

Step 4: Recovery Strategies

The objective of recovery strategies is to restore IT operations quickly and effectively following a disruption. A critical focus is to provide access to all sensitive information. Several factors will influence recovery strategy including cost, allowable outage time, security and integration with larger organizational level contingency plans.

The choice for the recovery approach would depend on the incident, type of system and its operational requirements. Technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, Uninterruptible Power Supply (UPS), and mirrored systems should be considered when developing a system recovery strategy.

Step 5: Development of Contingency Plan

The contingency plan contains detailed roles, responsibilities, teams, and procedures associated with restoring critical systems following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements.

Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach. The NIST identifies five main components of the contingency plan. They are:

1. Supporting Information
2. Notification/Activation Phase
3. Recovery Phase
4. Reconstitution Phase
5. Plan Appendices

Step 6: Testing and Training

Testing of the plan is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures.

Step 7: Review and Maintenance

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan.

Responsibilities:

The Security Officer is responsible for implementation of the Contingency Plan Policy. ~~leading compliance activities that bring Sweetwater County School District #1 into compliance with regulatory requirements in areas such as:~~

- ~~• Data backup plan~~
- ~~• Disaster recovery plan~~
- ~~• Emergency mode operation plan~~
- ~~• Testing and revision~~
- ~~• Application and data criticality analysis~~

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)