SWEETWATER COUNTY SCHOOL DISTRICT #1

Agenda Item 15-d

Security Incident Procedures

Security Incident Procedures

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:
The purpose is to address security incidents.

Sweetwater County School District #1 will create processes for the identification, reporting, and ensuring a timely response to real or potential violations of the security or a material breach of any part of the district's security policy.

Scope:
This policy applies to Sweetwater County School District #1 in its entirety, including all workforce members. In addition, some third parties such as contractors or vendors, may be required to abide by parts of this policy if required by Sweetwater County School District #1 in a memorandum of understanding.

Policy:
Sweetwater County School District #1 will maintain procedures for identifying security incidents. A security incident is any breach of security policy, or any activity that could potentially put sensitive information at risk of unauthorized use, disclosure, or modification.

A breach is defined as the unauthorized acquisition, access, use, or disclosure of protected information as defined below, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. If a breach has occurred, members of the workforce must immediately follow the instructions in the Data Breach Discovery Management Policy, policy # XXXX.

Incidents will be classified as "serious" or "non-serious." Non-serious incidents generally have the following characteristics:

- It is determined that there was no malicious intent (or the attack was not directed specifically at Sweetwater County School District #1) associated with the incident ~~and~~
- It is determined that no sensitive information was used, disclosed, or damaged in an unauthorized manner

Serious incidents generally have the following characteristics:

- It is determined that there was malicious intent and/or an attack was directed specifically at Sweetwater County School District #1
- It is determined that sensitive information, may have been used, disclosed, or damaged in an unauthorized manner or that this incident may be construed a data breach

All workforce members of Sweetwater County School District #1 will report any security incident to the Security Officer that they become aware of or suspect as soon as practical.

Sweetwater County School District #1 will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature.

Incidents characterized as serious by the Security Officer will be responded to immediately and reported to all upper-level administration.

Sweetwater County School District #1 will attempt to mitigate any harmful effects, when possible, where a security incident affects sensitive information.

Responsibilities:
All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Staying aware of and identifying potential security incidents
- Reporting any suspected security incident to the Security Officer
- Assisting the Security Officer in ending the security breach and mitigating its harmful effects, if possible

The Security Officer is responsible for:

- Maintaining all security incident-related policies and procedures
- Characterizing all reported security incidents as “serious” or “non-serious” as per the guidelines outlined above. The Security Officer may take into account their professional expertise and experiences when making these characterizations
- Maintaining procedures for responding to security incidents
- Documenting all reported security incidents and their outcome

The Security Officer and other members of management are jointly responsible for:

- Mitigating, to the extent possible, any harmful effects of security incidents
- Deciding when it is appropriate to contact law enforcement officials about a security incident that has been characterized as serious
- The Security Officer is responsible for leading compliance activities that bring Sweetwater County School District #1 into compliance with regulatory requirements.

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 Security Incident Response Policy include:

- Security Incident Response Procedure
- Security Incident Documentation Procedure

Form(s):
Forms related to the Assigned Security Responsibility Policy include:

- Security Incident Documentation Log

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