Data Breach Management

Purpose:
The Data Breach Management Policy is intended to assist employees responsible for managing breach related activities of Sweetwater County School District #1 when making decisions after a data breach has been identified. This policy is designed to minimize the loss and destruction of data, mitigate the weakness that was exploited and restore all computing and other impacted services to Sweetwater County School District #1.

Scope:
This policy applies to all Sweetwater County School District #1 workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Sweetwater County School District #1. More specifically, this policy applies to employees of Sweetwater County School District #1 that are responsible for the security of protected information.

Policy:
If a data breach is discovered at Sweetwater County School District #1 the following steps will be followed in order to prevent further damage, assess the severity of the breach, and manage all associated breach related activities.

- Once a breach has been identified, the Security Officer will assemble the Security Incident Response Team (SIRT) according to the Security Incident Procedures Policy GBCEI, develop a response according to the review the breach details and develop an appropriate response to prevent further data leakage, and assess the details of the breach.

- The Security Officer and the SIRT will manage all phases of the process once a breach has been identified.

- The Security Officer and the SIRT will keep Sweetwater County School District #1 leadership apprised of the situation.

- Priorities of the Security Officer and the SIRT will be:
    - Stopping the data leakage
    - Mitigation of the weakness, that was exploited
    - Restoration of normal business
    - Notification of persons and businesses impacted as deemed appropriate

- The Security Officer and SIRT will work with Sweetwater County School District #1 legal counsel to determine applicable state and federal laws that may be relevant to the incident; including but not limited to FERPA and state breach notification laws.

- Forensic analysis of the breach is to begin immediately upon determination of the breach, unless law enforcement deems a delay is appropriate, or additional forensic support is required beyond the Sweetwater County School District #1 Information Technology (IT) Team.

- All meeting minutes, technical documentation, and hand written notes of the breach are to be compiled by the Security Officer or designee within 72 hours of the closure of the breach.

- Any systems that were compromised or targeted as part of an incident resulting in an investigation may be quarantined as determined by the Security Officer and SIRT.

- Based upon the scope of the perceived threat the Security Officer and SIRT will notify local law enforcement, including but not limited to local police, sheriff's office and regional FBI office.

Responsibilities:
The Security Officer and (SIRT) are responsible for:

- The proper management of the security incident

All workforce members are responsible for:

- Following all security related policies and procedures

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): None

Form(s): None

References:

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

Adopted: 7/18/18