Information System Activity Review Policy

Purpose:
The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. A separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Scope:
This policy applies to Sweetwater County School District #1 in its entirety, including all systems that process sensitive information.

Policy:
Sweetwater County School District #1 will clearly identify all critical systems that process sensitive information and implement security procedures to regularly review the records of information system activity.

The information maintained in audit logs and access reports including security incident tracking reports must include if possible but is not limited to

- User IDs
- Dates and times of log-on and log-off
- Terminal identity, IP address and/or location
- Records of successful and rejected system access attempts

Safeguards must be deployed to protect against unauthorized changes and operational problems including but not limited to:

- The logging facility being deactivated
- Alterations to the message types that are recorded
- Log files being edited or deleted
- Log file media becoming exhausted, and either failing to record events or overwriting itself

Responsibilities:
The Security Officer will be responsible for the implementation of the Information System Activity Review 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):

- Security Incident Procedures

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: 05/14/18