File: EHAW

Wireless Security Policy

Purpose:

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of Sweetwater County School District #1's wireless infrastructure to a ***reasonable and appropriate level***.

Scope:

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

Policy:

Sweetwater County School District #1 wireless infrastructure must follow these guidelines:

Design

- Ensure that 128-bit or higher encryption is used for all wireless communication.
- Fully test and deploy software patches and updates on a regular basis.
- Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.

Access Points (AP)

- Maintain and update an inventory of all Access Points (AP) and wireless devices.
- The default settings on APs, such as those for SSIDs, must be changed.
- APs must be restored to the latest security settings when the reset functions are used.
- Turn on audit capabilities on AP; review log files on a regular basis.

Mobile Systems

- Install anti-virus software on all wireless clients.
- Disable file sharing between wireless clients.

Responsibilities:

The Security Officer has the responsibility to ensure implementation of the Wireless Security 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): 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: 8/13/18