Remote Access Policy

Purpose:
The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to Sweetwater County School District #1's enterprise 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. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

Policy:
The Sweetwater County School District #1 remote access infrastructure must follow these guidelines:

- It is the responsibility of district employees, contractors, vendors and agents with remote access privileges to the district network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
- Secure remote access must be strictly controlled. Control will be enforced by using strong passwords.
- At no time should any employee provide their login or e-mail password to anyone, not even family members.
- Employees and contractors with remote access privileges must ensure that their district-owned or personal computer or workstation, which is remotely connected to the district network, is not connected to any unsecured network at the same time, with the exception of personal networks that are under the complete control of the user.
- Employees and contractors with remote access privileges to the district network must not use non-district e-mail accounts (for example, Hotmail, Yahoo, AOL), or other external resources to conduct district business, thereby ensuring that official business is never confused with personal business.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by the Security Officer.
- All hosts that are connected to internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the district production network must obtain prior approval from the Security Officer.

Responsibilities:
The Security Officer is responsible for ensuring the implementation of the Remote Access 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: 05/14/18