SWEETWATER COUNTY SCHOOL DISTRICT #1

Agenda Item 12-b

Protection from Malicious Software Policy

Protection from Malicious Software Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:
The purpose is to implement procedures for guarding against, detecting, and reporting malicious software. Malicious software including but not limited to viruses, worms, Trojan horses and backdoor programs. ~~The key difference between the malicious software is their means of spreading.~~

Scope:
This policy applies to Sweetwater County School District #1 in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Policy:
Sweetwater County School District #1 will deploy malicious software checking programs at the perimeter ~~(edge)~~ of the network and on individual end-user systems.

Sweetwater County School District #1 will subscribe to receiving and deploying updates to malicious software checking programs.

Sweetwater County School District #1 will conduct security training that will include information about:

- Potential harm that can be caused by malicious software
- Prevention of malicious software such as viruses
- Steps to take if a malicious software such as a virus is detected

Responsibilities:
The Security Officer is responsible for ensuring that malicious software checking programs are installed both on the perimeter of the network and on individual end-user systems. The Security Officer will identify all critical systems and network components that are vulnerable to malicious software. All such identified systems will have malicious software checking capability.

Members of the workforce must not configure or introduce any modifications to systems or applications to prevent the execution of malicious software checking programs. Members of the workforce that suspect any malicious software infection must immediately contact the Security Officer or their supervisor by phone or walk-in – not by e-mail – about the suspected threat.

Members of the workforce must participate in all security awareness training programs and apply the knowledge in preventing, detecting, containing and eradicating malicious software.

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).