



**SWEETWATER COUNTY
SCHOOL DISTRICT #1**

Agenda Item 12-c

Password Management Policy

Password Management Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to implement procedures for creating, changing and safeguarding passwords.

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 requires that:

- All passwords must be changed at least once every 90 days.
- All production system-level passwords must be part of the Security Officer's administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

Users must select strong passwords. Strong passwords generally have the following characteristics:

- Be at least eight characters in length
- Be a mixture of letters and numbers
- Be changed at least every 90 days
- Be different from the previous 6 passwords
- Not contain 4 consecutive characters used from the previous password
- Not contain the user's user id

Note that poor weak passwords generally have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, and so on
 - Computer terms and names, commands, sites, companies, hardware, software
 - Birthdays and other personal information such as addresses and phone numbers
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, and so on
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (for example, secret1, 1secret)

Members of the workforce must follow these guidelines for passwords:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an e-mail message

- Don't talk about a password in front of others
- Don't hint at the format of a password, like, "my family name"
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers

If someone demands a password, refer them to this document or have them call someone in the Information Technology department or contact the Security Officer.

~~Members of the workforce must not use the "Remember Password" feature of applications (PowerSchool, Outlook Web Access, Alico, and so on).~~

Computers left unattended must be put to sleep or have the screensaver enabled and require a password to gain access to the device.

Members of the workforce must not write passwords down and store them. ~~anywhere in your office.~~ Further, passwords must not be stored on ANY computer system or mobile devices (including Palm Pilots or similar devices) without encryption.

Responsibilities:

The Security Officer is responsible for ensuring the implementation of the Password Management Policy.

~~Password cracking or guessing may be authorized to be performed on a periodic or random basis by the Security Officer. If a password is guessed or cracked during one of these scans, the user will be required to change it.~~

~~Members of the workforce must not share their passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.~~

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).