

TECHNOLOGY - Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Grand County School District's (hereafter known as GCSD) entire network. As such, all GCSD computer users (including contractors and vendors with access to GCSD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any GCSD facility, has access to the GCSD network, or stores any non-public GCSD information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the GCSD's Technology Office administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least once a year, at the beginning of school year. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user where practical.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at GCSD. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight 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, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words " Grand County School District ", "Moab", "gcsd" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:;'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for GCSD accounts as for other non-GCSD access (e.g., personal ISP account, option trading, benefits, etc.).

Do not share GCSD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential GCSD information.

C. Password Guidelines

Here is a list of things NOT to do:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "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 while on vacation

If someone demands a password, refer them to this document or have them call someone in the GCSD Technology Office.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger). Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If you suspect an account or password has been compromised, report the incident to GCSD's Technology Office and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by GCSD's Technology Office or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5.0 Enforcement

Any computer user found to have violated this policy may be subject to disciplinary action.

6.0 Definitions

| Term | Definition |
|------------------------------------|--|
| Application Administration Account | Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator) |
| "sudo" | a program that allows a normal user access to administrative software |
| SNMP | a type of management software used on the network by the Technology Office |