Provo City School District Technology Security Policy

Password Procedure

Last Update Status: *Updated January 2015*

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the entire network. This guideline provides best practices for creating secure passwords.

2. Purpose

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

3. Scope/Responsibility

This procedure applies to all personnel and entities working on behalf of the district, who have or are responsible for any account (or any form of access that supports or requires a password) on any system that resides at or is connected to any PCSD facility.

4. Procedure

To minimize the possibility of unauthorized access, all passwords should meet or exceed the guidelines for creating strong passwords.

- **Password Characteristics:**
  Strong passwords
  - Contain at least 12 alphanumeric characters
  - Contain both upper and lower case letters
  - Contain at least one number (for example, 0-9)
  - Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

  Poor or weak passwords
  - Contain less than eight characters
  - Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon
  - Contain personal information such as birth dates, addresses, phone numbers, names of family members, pets, friends, and fantasy characters
  - Contain work-related information such as building names, mascots, hardware, or software
  - Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321
  - Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret)
  - Are some version of "Welcome123" "Password123" "Changeme123"
  - Users must not use the same password for PCSD accounts as for other non-PCSD access

(for example, personal email accounts, shopping sites, social media, and so on)

- Where possible, users must not use the same password for various PCSD access needs
- User accounts that have system-level privileges granted through group memberships or programs such as PowerSchool must have a unique password from all other accounts held by that user to access system-level privileges; unless account has 2-factor authentication enabled
- You should never write down or store passwords without acceptable encryption. Instead, try to create passwords that can be remembered easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R!
- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually. The recommended change interval is every four months
- Password cracking or guessing may be performed on a periodic or random basis by the InfoSec team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it
- Systems that can force password change must force regular password changes
- Default passwords must be changed during initial setup and configuration
- The Technology help desk manages forgotten passwords and password resets. Be prepared to answer some questions to verify your identity.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information
- Passwords must not be inserted along with the username into email messages or other forms of electronic communication
- Do not reveal a password on questionnaires or security forms
- Do not hint at the format of a password (for example, "my family name")
- Do not share your PCSD passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) *without* encryption
- Never use the "Remember Password" feature of applications (for example, web browsers)
- Any user suspecting that his/her password may have been compromised must report the incident to their supervisor and change all passwords immediately
- Use Auto-logout on systems that allow it