Overview

Passwords are an important aspect of network and computer security and a fundamental necessity for safeguarding information. Consistency and reliability are paramount for the CASD network to serve its users. A poorly chosen password may result in the compromise of the entire computer network of the Chambersburg Area School District. According to Policy 815, The District’s Acceptable Use Policy, “Users are required to use unique strong passwords that comply with the School District’s password, authentication, and syntax requirements.” As such, all District authorized account owners (including employees, students, parents, contractors and vendors with access to District systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All passwords are to be treated as sensitive, confidential District information.

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.

Scope

The scope of this policy includes all authorized account owners who have been provided an account on any computer that resides at any District building, or has access to the District network.

Definitions

Every user should be aware of how to select and use strong passwords. Users must not use weak passwords.

Strong passwords:

- 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!@#$%^&*()_+|~=`\[]:";)
- 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.

Weak passwords:

- contain less than eight characters
- are found in a dictionary (English or foreign)
- are common usage words such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word, keyboard, or number patterns like aaabb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards or followed by a digit (e.g., secret1)

Responsibilities

- All staff passwords must be changed every 180 days.
• All passwords must be a minimum of 8 characters in length and be uniquely constructed to contain both letters AND numbers.
• All staff passwords must conform to the guidelines and standards described below.

Requirements:

All passwords must be at least 8 characters long and:
• Does not contain your username, real name and/or company name
• Is significantly different from previous passwords
• Contains characters from three of the following four groups:
  o Uppercase characters (A–Z)
  o Lowercase characters (a–z)
  o Numerals (0–9)
  o Symbols (all keyboard characters not defined as letters or numerals)

Passwords must be changed every 180 days enforced by server policy (or as required by the individual program) by the user to maintain systems’ security. All passwords are to be treated as sensitive and confidential. Users may change their password at any time. If security is compromised, immediately notify CASD’s Technology Department.

After 3 unsuccessful computer login attempts, the user will be locked out and the user will need to wait 30 minutes until they are unlocked or contact the CASD Technology Department (Building Helpdesk at Secondary Buildings) to unlock their account and reset the password.

Each authorized user will be responsible for use of the computer equipment to protect all data files and computer programs, by logging off or locking the system before leaving their workstation. All computing equipment must be shutdown at the end of each work day, on weekends, on days off, and during all vacations.

Training will take place to demonstrate the change of passwords, suggest creation of complex passwords, how to secure passwords, and which applications password changes will affect.

Application Development Standards

Application developers must ensure that their programs:

• support authentication of individual users, not groups.
• do not store passwords in clear text or in any easily reversible form.
• meet standards utilized in District applications or SSO package.

Enforcement

All user accounts provided are a privilege and the District reserves the right to revoke that privilege at any time.

Any user who violates this policy may be subject to appropriate disciplinary action per the District’s Acceptable Use Policy.