Catalina Foothills Unified School District #16

Password Guidelines

Purpose:

This document is intended to define optimal business practices for user passwords in Catalina Foothills School District (CFSD). Wherever possible, secure passwords must be used to protect network resources, network access, financial data, personnel data, student information, and any other resource deemed critical by CFSD. This document should provide general guidance in constructing a secure and appropriate password, as well as define password requirements for common systems.

Scope:

All CFSD staff and students should follow the guidelines to ensure the security of CFSD resources and personal data. Third party vendors, contractors, and subcontractors should be expected to use secure and appropriate passwords.

Some CFSD systems have password requirements set by the vendor, with little configuration permitted by the CFSD IT Department. In each case, requirements specific to that vendor should be adhered to.

When possible, the CFSD IT Department will set minimum password standards for system access. Users are encouraged to create highly complex passwords, but the minimum standards must be observed.

Password Standards:

Many CFSD systems have specific password requirements, as detailed in the section "Minimum Password Requirements for Specific CFSD Applications". For all other systems, the following best practices should be observed:

- A password should be at least eight (8) characters in length.
- A password should contain at least three (3) of the following character types:
    - Uppercase letters

    - Lowercase letters
    - Numbers
    - Special characters, such as !@#$%^&*()-=?;:
- A space character should not be used.
- A password should not be similar to the user's five most recent passwords.
- A password should not contain the user name.
- A password should not be a dictionary word.

Password Protection:

Every user should make every effort to protect their password. Compromise of a user password may enable access to CFSD systems, but could also jeopardize the user's personal and confidential information. All users should take the following measures to protect their passwords:

- Do not use the same password for CFSD accounts and personal accounts.
- Do not share a password over the phone.
- Do not share a password in an email.
- Do not give hints regarding the format of your password.
- Do not share a password in any paper or online form.
- Do not write passwords down or try to hide them (such as under the keyboard).
- Do not store passwords in any unencrypted file.
- Do not utilize the "Save Password" feature of applications or web browsers.

Minimum Password Requirements for Specific CFSD Applications:

MUNIS:

MUNIS passwords must be at least eight (8) characters, with at least one (1) number or special character, at least one (1) lowercase letter, and at least one (1) uppercase letter. The system forces a password change every 90 days, and a user may not re-use any of their last five (5) passwords.

Active Directory/Computer Login:

Active Directory and computer login passwords must be at least eight (8) characters, with at least one (1) number, and at least one (1) capital letter. Passwords must be changed yearly.

Staff Google Accounts:

Google "G Suite" accounts for CFSD staff members must have passwords that are at least eight (8) characters, with at least one (1) lowercase letter, at least one (1) uppercase letter, at least one (1) number, and at least one (1) special character. Passwords must be changed every 120 days, and a user may not re-use any of their last five (5) passwords.

Synergy Accounts:

Synergy user accounts must have passwords that are at least eight (8) characters and contain both letters and numbers. A user may not re-use any of their last five (5) passwords.