IT7
CATEGORY: INFORMATION TECHNOLOGY

LOGIN AND PASSWORD SECURITY POLICY

I. PURPOSE

Promote a secure computing environment throughout Central Coast Community Energy's (CCCE) information services and systems by establishing standards for managing login accounts and strengthening login security.

II. SCOPE

This policy is applicable to all users 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 CCCE facility, has access to the CCCE network, resides on third party servers (Office 365, etc.), or stores any non-public CCCE information.

III. DEFINITIONS

"**Multi-Factor Authentication**" (MFA) increases the security of user logins above and beyond just a password. With MFA, users are required to acknowledge a phone call, text message, or an app notification after correctly entering their password.

"**Passphrase**" passphrase is a kind of password that uses a series of words, separated by spaces or not (it doesn't really matter). Although passphrases often contain more characters than passwords do, passphrases are usually less complex (four words instead of, say, 12 random characters). This makes passphrases easier to remember while providing greater security against dictionary attacks.

"**Windows Hello**" is a more personal, more secure way to get instant access to your Windows 10 devices using a PIN, facial recognition, or fingerprint. You'll need to set up a PIN as part of setting up fingerprint or facial recognition sign-in, but you can also sign in with just your PIN. Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices.

IV. POLICY

Where technically and operationally feasible, the following account and password/passphrase management and multi-factor authentication practices must be followed:

A. METHODS

- Whenever possible, for all systems, services, or subscriptions (not just Microsoft), setup Multi-Factor Authentication (MFA) in combination with a strong password. Including:
  - Windows Hello Logins
  - Text messaging MFA
  - Alternate e-mail MFA

B. PASSWORD CREATION AND CHANGE

- A password is required for all login accounts and each must conform to the Password Construction Guidelines attached.
- Password is changeable by user.
- Password must be changed at least every 90 days.
- A new password cannot be the same as any of the last four used for that account.
- Password cracking or guessing may be performed on a periodic or random basis by the IT staff. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. WINDOWS HELLO

- Windows Hello should be setup whenever possible.
- PIN is changeable by user.
- PIN must be changed at least every 90 days.
- Fingerprint and Facial Recognition are allowed for Windows Hello after PIN setup.
- It is recommended that you use a unique PIN for each Windows device.
- The PIN must be at least 6 characters. Alphanumeric options are allowed.
- PINs cannot be shared.

D. PASSWORD PROTECTION

- The login account is unique and is assigned to an individual user. A login account cannot be shared.
- If an administrator password is required by a supplier for troubleshooting or an upgrade, IT staff will not disclose the password but must input it to the required system himself/herself. If a password is disclosed, IT staff must change it as soon as possible.
- An administrator-level account cannot be shared. Multiple administrator accounts are required for multiple administrator-level personnel.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential CCCE information.
- Do not reveal a password on questionnaires or security forms.
- 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 device (phone, tablet) without encryption.
- Any user suspecting that their password may have been compromised must report the incident to IT staff and change all passwords.

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

IT staff will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. NON-COMPLIANCE

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

VI. ATTACHMENT: PASSWORD CONTRUCTION GUIDELINES

PASSWORD CONSTRUCTION GUIDELINES

OVERVIEW

Passwords are a critical component of information security. They serve to protect user accounts. However, poorly formed passwords result in the compromise of individual systems, data, or the CCCE network. These guidelines provide best practices.

SCOPE

These guidelines apply to employees, contractors, consultants, temporary and other workers at CCCE. These guidelines apply to all passwords including but not limited to user-level accounts, system- level accounts, web accounts, service or subscription accounts, and e-mail accounts.

STATEMENT OF GUIDELINES

All passwords / passphrases should meet or exceed the following guidelines whenever possible:

STRONG PASSWORDS / PASSPHRASES HAVE THE FOLLOWING CHARACTERISTICS:

- Contain at least 16 alphanumeric characters.
  Note: 12 or more characters are considered strong when all four character types are used.
- Contain at least three difference character types:
  - Upper-case Letters
  - Lower-case Letters
  - Numbers (for example, 0-9)
  - Special characters (for example, #$?!)

POOR OR WEAK PASSWORDS HAVE THE FOLLOWING CHARACTERISTICS:

- Contain less than twelve characters.
- Can be found in a dictionary or exists in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone number, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, 123321, etc.
- Are some version of “Welcome123”, “Password123”, etc.
- Contain common words spelled backward, preceded by or followed by a number (for example, terces, secret1 or 1secret).

PASSPHRASES

Wherever possible, a passphrase is the recommended method for login credentials. Strong passphrases should follow the general password construction guidelines and include upper and lower case letters, and numbers and/or special characters.

- The more words, the stronger the passphrase. Five words are better than 4.
- Common phrases you use are not recommended. The more random, the better.