COMMUNITY FOUNDATION of Northeast Alabama

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the Community Foundation of Northeast Alabama's (CFNEA) resources. All users, including staff, trustees, interns and volunteers with access to the Foundation's 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 the 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 CFNEA facility, has access to the CFNEA network, or stores any non-public CFNEA information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed every six months in January and July.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every six months in January and July.
- All user-level and system-level passwords must conform to the guidelines described below. Everyone is required to use strong passwords.

4.2 Guidelines

A. General Password Construction Guidelines

All users at CFNEA should be aware of how to select strong passwords.

Strong passwords contain at least 23 characters with either spaces or underlines.

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 password might be: "This May Be One Way To Remember".

(NOTE: Do not use this example as a password!)

B. Password Protection Standards

- Always use different passwords for CFNEA accounts from other non-CFNEA access (e.g., personal ISP account, IRA trading, benefits, etc.).
- Always use different passwords for various CFNEA access needs whenever possible. For example, select one password for logging on and another for Community Suite/GLM/SLM.
- Do not share CFNEA passwords with anyone outside CFNEA. All passwords are to be treated as sensitive, confidential CFNEA information.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the President & CEO.
- Always decline the use of the "Remember Password" feature of applications. (e.g., Eudora, OutLook, Netscape Messenger).

If an account or password compromise is suspected, report the incident to the President & CEO immediately.

C. Use of Passwords and Passphrases for Remote Access Users

Access to the CFNEA network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

D. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@GreatToSeeYou*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

E. <u>Two-Factor Authentication</u>

Two-factor authentication adds an extra layer of security for computer programs and digital devices. CFNEA staff must connect their accounts (email, C-Suite, Windows, etc.) to a second method of confirming the users' identity besides a log-in username and password. The second method in this two-step process can take the form of a physical device (a USB security key or a Bluetooth security key), confirmation of a digital prompt sent to a mobile phone, or entering a code sent to a mobile phone by either text or phone call.

F. <u>Email</u> Encryption

To add enhanced security to CFNEA emails, users may employ Microsoft Outlook's encryption option via S/MIME or Gmail's confidential mode to help protect sensitive information from unauthorized access. However, be aware that encryption methods do not prevent recipients from taking screenshots or photos of your messages or attachments.

5.0 Enforcement

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

6.0 Revision History

Approved by the Board of Trustees February 13, 2014
Approved by the Board of Trustees August 8, 2019
Approved by the Board of Trustees November 21, 2019

ACKNOWLEDGMENT

I have read the *Password Policy*. I understand the contents, and I agree to comply with said *Policy*.

Signature _____

Name _____Date _____