Vermont Educational and Health Buildings Financing Agency

Computer Password Policy

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the VEHBFA's resources. All users, including contractors and vendors with access to VEHBFA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Scope

The scope of this policy includes all personnel and consultants 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 a VEHBFA facility.

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.

General

All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed on at least a quarterly basis.

Password Construction Guidelines

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

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
  - o Lower case characters
  - o Upper case characters
  - o Numbers
  - o Punctuation
  - o "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least nine alphanumeric characters.
- Weak passwords have the following characteristics:
  - The password contains less than nine characters
  - The password is a word found in a dictionary (English or foreign)

- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Vermont Educational and Health Buildings Financing Agency, "VEHBFA", or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

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 phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

(NOTE: Do not use either of these examples as passwords!)

Password Protection Standards

- Do not share VEHBFA passwords with non-employees. All passwords are to be treated as sensitive, confidential VEHBFA information.
- Passwords should never be written down or stored on-line without encryption.
- 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 Executive Director.
- 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 Executive Director or the network administrator.

Use of Passwords and Passphrases for Remote Access Users

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

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*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

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

Adopted: February 13, 2012