Computer Passwords Policy

Objective

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of [Company Name]'s entire corporate network. As such, all [Company Name] employees (including contractors and vendors with access to [Company Name] systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This policy establishes a standard for the creation of strong passwords, the protection of those passwords and the frequency of change.

Scope

The scope of this policy includes all employees 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 [Company Name] facility, who have access to the [Company Name] network, or who store any nonpublic [Company Name] information.

User Authentication

Every user must be assigned a unique user account (user ID) and a password for access to [Company Name] systems. Shared or group user IDs are prohibited for user-level access. Systems and applications must authenticate using a password or token entry. The use of nonauthenticated user IDs (i.e., those without passwords) or user IDs not associated with a single identified user are prohibited. The account will lock a user out after six invalid login attempts within 30 minutes. Locked accounts shall remain locked for at least 30 minutes or until the System Administrator unlocks the account. Users may contact the IT Service Desk to have their account unlocked. Multifactor authentication is required for all users accessing [Company Name] systems remotely.

Password Management

Passwords must be created and managed in accordance with this section.

Password Requirements

- All user-level [Company Name] network passwords will expire every 90 days and must be changed.
- New passwords cannot be the same as the previous four passwords.
- Passwords must be at least eight characters in length. Longer is better.

- Passwords must contain both uppercase and lowercase characters (e.g., a-z and A-Z).
- Passwords must contain at least one number (e.g., 0-9).
- Accounts shall be locked after six failed login attempts within 30 minutes and shall remain locked for at least 30 minutes or until the System Administrator unlocks the account.

To unlock an account or change a password without logging in, some [Company Name] systems require the Technology Department to provide a new temporary password to the user. In such cases, passwords must be provided verbally and the user must immediately log in and change the account password.

Passwords should not be shared with anyone, including IT support personnel, unless approved by the IT Security Specialist.

All passwords are to be treated as sensitive, confidential information. If someone requests your password(s), please inform him or her that you cannot provide that information per [Company Name] policy and contact the IT Security Specialist about the request. If you suspect an account or password has been compromised, report the incident immediately and change all related passwords.

The Technology Department or authorized outside "penetration testers" may perform password cracking or guessing on a periodic or random basis to test the security of the [Company Name] network. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking and guessing are not to be performed by anyone outside of the Technology Department or an approved third-party auditor.

The Technology Department strongly encourages the use of a password manager program to help ensure that all passwords are strong, unique and easily changed. Users should open an IT Service Desk ticket with a request for more information on password managers allowed on the [Company Name] network and for assistance in getting the password manager installed and configured on their computer.

Guidelines for Password Construction

A strong password:

- Contains both uppercase and lowercase characters (e.g., a-z and A-Z).
- Contains digits and punctuation characters (e.g., 0-9 and !@#$%^&*).
- Is at least 8-15 alphanumeric characters long and is a passphrase (e.g., "Ohmy1stubbedmyt0e").
- Is not a single word in any language, slang, dialect or jargon (e.g., "password" or "Fluffy").
- Is not based on personal information, names of family members, etc.

Passwords should never be written down or stored online. Employees should try to create passwords that can be easily remembered. One way to do this is to 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.

Use of Passwords and Passphrases for Remote Access Users

Access to the [Company Name] 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.

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 uppercase and lowercase letters as well as numeric and punctuation characters. An example of a good passphrase is "Vaca@The#OBX!$MyDreamin!"

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

Enforcement

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