Password Policy

Overview

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

The President/Superintendent or designee shall have the authority to enforce guidelines set forth below.

Purpose

This policy establishes standards for the creation of strong passwords, the protection of those passwords, and the frequency of change. This policy complements AP 3720 – Acceptable Use Policy.

Scope

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 IVC system.

Passwords

IVC uses passwords to allow employees to access computer systems and resources. Some of the more common uses include user-level accounts, computer login, e-mail accounts, screen saver protection, voicemail password, and equipment logins. Everyone should be aware of how to select strong passwords. When possible, IVC will integrate systems so that the primary user-level account can provide access to multiple authorized systems using Single Sign-On (SSO). Because these systems are often integrated, a single password may provide access to multiple systems making password security and protection a critical priority.

A. Password Requirements

- All user-level passwords must have a minimum of 8 characters in length.
- All users with elevated privileges must have a minimum of 12 characters in length.
- All passwords must contain characters from three of the following categories:
    - Uppercase letters
    - Lowercase letters
    - Base 10 digits (0 through 9)
    - Special character
- System will not allow the reuse of the previous 3 passwords.

B. Password Expiration

C. ~~All passwords to access IVC systems will expire in 12 months from the last effective change. After twelve months, system users will need to change their password. Employees cannot reuse the same or previous 3 passwords. Employees with elevated privileges cannot reuse the same or previous 5 passwords.~~ To encourage the use of more complicated passwords IVC is not implementing a password expiration period. If a users password is flagged for being weak or compromised their password will be required to be changed. Employees cannot reuse the same or previous 3 passwords.

A weak password is one that does not comply with this password policy.

A compromised password is one that has been disclosed in public breaches that are identified in the Pwned Passwords Database.

D. Password Reset

IVC system users can change their password at any time of the year if they believe their password has been compromised or have a desire to change it. The password reset tool allows users to change their IVC primary account password. The password reset tool can be found online at https://www.imperial.edu/faculty-and-staff/password-reset-tool/.

E. Password Protection Standards

- Do not use the same password for IVC accounts as for other non-IVC access (e.g., personal ISP account, online banking, social media sites). Where possible, don't use the same password for various IVC access needs.
- Do not share IVC passwords with anyone, including work colleagues. All passwords are sensitive, confidential IVC information.
- Do not write passwords in e-mail or text messages or other forms of electronic communication (social media, group chat).
- Do not write down passwords and place in visible areas or inconspicuous areas of the workstation (e.g., under the keyboard).
- IVC strongly encourages the use of "three random words" for your password, https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words
- IVC encourages the use of password managers or secure software applications that serve as password vaults to secure multiple account passwords.
- IVC encourages employees to change their passwords frequently, especially if the employee suspects their password has been compromised or shared.

Elevated Privileges

Elevated privileges refer to user accounts that are responsible for performing administrative functions on applications and/or equipment. User accounts with elevated privileges require additional security controls to minimize further risk of being compromised, such as a password with a 12-character length. Users that have elevated privileges must use multi-factor authentication.

Multi-Factor Authentication

Multi-Factor Authentication, or MFA, is an enhanced form of user authentication. In addition to entering a username and password, MFA requires an additional form of authentication such as entering a one-time token. IVC provides the token through a third-party application or a text message. IVC may enforce MFA under the following circumstances:

- User account requires elevated privileges to manage IVC computer systems (to include local computer)
- User account has a history of being compromised
- User accounts that are favorable targets for malicious activity
- Users that manage personal identifiable or sensitive information for the organization
- Other circumstances where increased security is important

New IVC Employees

During the employee hiring process, new IVC employees will be provided an initial password. When you log into your account for the first time you will be required to set a new user-level password for their IVC primary account.

Definitions

User-level Password: All IVC system users will be assigned a user account that requires a User-level password. This password authenticates users and allows access to computers, wireless networks, e-mail, and other resources provided by IVC.

System-level Password: Certain employees within IVC will be managing systems that require an elevated privileged account, such as a System-level password. These passwords have more stringent security requirements.

Password Manager: Refers to a tool or application to store numerous passwords or account information in encrypted form.

Single Sign-on (SSO): Refers to systems or applications that integrate with the IVC employee directory system. Systems that support SSO allow IVC employees to use their primary account to login to applications and systems. Where possible, IVC will integrate applications and systems to minimize the number of accounts provided to employees.

Three Random Words (https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words): This is a password philosophy that by combining three random words – you can create a password that's random enough to keep the bad guys out, but also easy enough to remember.