Password Policy

Overview

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

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.

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 MIoD facility, has access to the MIoD network, or stores any non-public MIoD information.

Policy

General

- All user-level passwords (e.g. email, web, desktop computer, CRM etc.) must be changed at least every six months.
- User accounts that have system-level privileges granted through programmes such as "Pastel and CRM" must have a unique password from all other accounts held by that user.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

General Password Construction Guidelines

All users at MIoD 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:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation

- "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)

- ❖ Contain at least 8 alphanumeric characters.

Weak passwords have the following characteristics:

- ❖ The password contains less than 8 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 "MIoD", 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)

Password Protection Standards

- Always use different passwords for <Company Name> accounts from other non-MIoD access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various MIoD access needs whenever possible.
- Do not share MIoD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential MIoD 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 an account or password compromise is suspected, report the incident to the CEO.

Use of Passwords and Passphrases for Remote Access Users

Access to the MIoD 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.

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

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the MIoD IT Security only. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Change Management

ITEM	FREQUENCY TO CHANGE PASSWORD	DATE OF LAST CHANGE
PC	Every 3 months	
CRM	Every 3 months	
WEBSITE	Every 3 months	
EMAIL	3 months	
MOBILE PHONES	One off	
TABLETS	One off	
PASTEL SOFTWARE	Every 6 months	
TEAMVIEWER	Every 6 months	
WIFI AND ROUTER	Every 6 months	

Responsibility

It is the responsibility of every user to change their password and the responsibility of the Accounts and Administration Coordinator to send a timely reminder and ensure that this policy is implemented.