JMTCPA Password Policy

Overview

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 a compromise of JMTCPA's entire network. As such, all JMTCPA employees (including contractors and vendors with access to JMTCPA systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

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.

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 JMTCPA facility, or has access to the JMTCPA network.

Policy

General

All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

• All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 10 passwords.

• Passwords must not be inserted into email messages or other forms of electronic communication.

• All user-level, system-level, and network access level passwords must conform to the guidelines described below.

Guidelines Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems.

ii. Not be a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 90 calendar days.

v. Not be identical to the previous ten (10) passwords.

vi. Not be transmitted in the clear or plaintext outside the secure location.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized user.

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
    - Default passwords shall be changed immediately on all equipment.

Password Protection Standards

Do not use your User ID as your password. Do not share JMTCPA passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential JMTCPA information. Here is a list of “do not’s”

- Don’t reveal a password over the phone to anyone
- Don’t reveal a password in an email message
- Don’t reveal a password to the boss
- Don’ talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with family members
- Don’t reveal a password to a co-worker while on vacation
- Don’t use the "Remember Password" feature of applications
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY computer system unencrypted.