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 Washington Township's entire network. As such, all Township employees (including contractors and vendors with access to Township 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 Washington Township facility, has access to the Washington Township's network.

Policy

General

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 180 days.
- All production system-level passwords must be part of the "Credentials" tab found in the "IP and vLAN Configurations" notebook.
- 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 be encrypted when sent using email messages or other forms of electronic communication.

Guidelines

Password Construction Requirements

i) Be a minimum length of eight (12) characters on all systems.
ii) Not be the same as the User ID.
iii) Expire within a maximum of 90 calendar days.
iv) Not be identical to the previous ten (10) passwords.
v) Not contain words located in the password exclusion list.
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, changed 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.
- Contractor accounts, when no longer needed to perform their duties.

When an account is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her Township point-of-contact (POC).
- Supervisor or POC should fill out a help desk ticket with the account information to be removed/changed.
- Upon notification, IT will then change/delete the user's password and delete or disable the user's account.

Password Protection Standards

Do not use your User ID as your password. Do not share Township passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Township 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 mail 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.

If an account or password is suspected to have been compromised, report the incident to the Information Systems Director or POC and change all passwords.

Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password.
- Should support Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

Remote Access Users

Access to the Township's networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required). Multi-Factor Authentication is required for all users accessing the Township's networks remotely.

Penalties

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