Table of Contents

1. Overview

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

2. Purpose

The purpose of this document is to establish standards for, creation of passwords, protection of passwords, and frequency of change of passwords.

3. Scope

This policy includes 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 organization facility, has access to any network, or stores any non-public information.

4. Procedures

4.1. Guidelines

4.1.1. General Password Construction Guidelines

Users should select strong passwords.

Strong passwords have the following characteristics:

- Contain all the following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - "Special" characters (e.g. @#$%^*()_+|~-=\`{}[]:";'<>/ etc.).
- Consist of at least ten characters.

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.

Passphrases are another example of a strong password. 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 password cracking tools. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "Tr@ff1c0n66WP00rTh1sM@rn1ng". This translates the traffic on 66 West was Poor This Morning.

(NOTE: Do not use either of these examples as passwords as they are now public domain!)

- If an account or password compromise is suspected, users should change their password and report the incident to the systems contact, organization, or systems owner.

- All production system-level passwords must be part of the InfoSec administered global password management database or similar “fire call” system (Break Glass Process). Normally these have non expiring passwords and setup by sys admins. They are easily forgotten or the person who set them is no longer available. A documented retrieval process should be maintained in case the password is needed to modify their service settings.

- Where Simple Network Management Protocol is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- Initial and reset (temporary) passwords shall be strong and unique.

4.1.2. Account Password Policy Settings

- Enforce Password History 24 Passwords remembered
- Minimum Password Age 5 Days
- Maximum Password Age 90 Days
- Minimum Password Length 10 Characters
- Password must meet complexity requirements Enabled
- Store password using reversible encryption Disabled

4.1.3. Account Lockout Policy Settings

- Account Lockout Duration 60 Minutes
- Account Lockout Threshold 5 Invalid logon attempts
- Reset account lockout counter after 30 Minutes

4.1.4. Audit Policy Settings

- All servers except Print and Proxy Servers
  - Audit account logon events Success, Failure
  - Audit account management Success, Failure
  - Audit directory service access Failure
  - Audit logon events Success, Failure
  - Audit object access Failure
  - Audit policy change Success, Failure
  - Audit privilege use Failure
  - Audit process tracking No Auditing
  - Audit system events Success, Failure

- All Print and Proxy Servers
  - Audit account logon events Failure
  - Audit account management Success, Failure
  - Audit directory service access Failure
  - Audit logon events Failure
  - Audit object access Failure
  - Audit policy change Success, Failure
  - Audit privilege use Failure
  - Audit process tracking No Auditing
  - Audit system events Success, Failure

4.1.5. Application Development Standards

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

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support TACACS+, RADIUS and/or X.509 with LDAP security retrieval wherever possible.
- Password should be encrypted.

4.1.6. Local Administrator Passwords

- Rename the Administrator account
- Local Administrator Accounts shall be separate from Domain Administrator Accounts
- Passwords are to be 12 characters, strong, and random or a passphrase

5. Basic Rules

- Don’t share your password
- Don’t write down your password and store on a Post-it next to your computer