Password Construction Guidelines

1.0 Purpose

Passwords are a fundamental component of information security, acting as the first line of defense for user accounts, systems, and data. Weak or easily guessable passwords significantly increase the risk of unauthorized access and compromise. The purpose of these guidelines is to provide clear best practices for creating and managing strong, secure passwords and passphrases to protect individual users and organizational assets.

2.0 Scope

These guidelines apply to all employees, contractors, consultants, temporary staff, vendors, agents, and other workers, including personnel affiliated with third parties, who are granted access to organizational systems or data. They apply to all passwords used for authentication, including but not limited to user-level accounts, system-level accounts (where applicable), web application accounts, email accounts, screen saver locks, voicemail access, network device logins, and any other system requiring password authentication within the organizational context.

3.0 Guideline Statements: Creating Strong Passwords and Passphrases

To enhance security, all passwords created and used for organizational accounts should adhere to the following principles:

3.1 Length:

*   **Minimum Length:** Passwords should be significantly long to resist brute-force attacks. A minimum length of **14 characters** is strongly recommended for all new passwords. Longer is generally better.
*   **Passphrases Encouraged:** Using **passphrases** (multiple words forming a memorable phrase) is highly encouraged. Examples: `"ItsTime4MyVaca!"`, `"Block-Curious-Sunny-L3aves"`. Passphrases can be easier to remember and type while meeting length and complexity requirements.

3.2 Complexity and Content:

*   Passwords should ideally incorporate a mix of character types (uppercase letters, lowercase letters, numbers, symbols). However, length is the most critical factor. A long passphrase without complex substitutions is often stronger than a short, complex password.

*   **Avoid Weak Content:** Passwords **must not** contain easily guessable information or predictable patterns. Avoid:
    *   Personal information (names of family, pets, friends; birthdates; addresses; phone numbers; usernames; real words directly related to you or the organization).
    *   Common keyboard patterns (e.g., `qwerty`, `asdfgh`, `12345678`).
    *   Repeating characters or simple sequences (e.g., `aaaaaa`, `111111`, `abcde`).
    *   Commonly used default or weak passwords (e.g., `Password123`, `Welcome1`, `Changeme`).
    *   Dictionary words spelled forwards or backward.

3.3 Uniqueness:

*   **Unique Passwords:** Each account (work-related or personal accounts accessed via work devices/networks) should have a **unique password**. Reusing passwords across different services dramatically increases risk; if one account is compromised, others using the same password become vulnerable.

4.0 Tools and Best Practices for Password Management

4.1 Password Managers:

*   Creating and remembering unique, strong passwords for every account is challenging. The use of organization-approved **password manager software** is highly encouraged. These tools securely store complex passwords and can help generate strong, random ones, requiring you only to remember one strong master password for the manager itself. Only use password managers vetted and approved by the designated IT authority (e.g., Precision Computer).

4.2 Multi-Factor Authentication (MFA):

*   Passwords alone are often insufficient. Wherever possible, **Multi-Factor Authentication (MFA)** must be enabled on accounts. MFA adds a crucial layer of security by requiring a second form of verification (e.g., a code from a mobile app, a text message, a hardware token) in addition to the password.

5.0 Compliance

5.1 Compliance Measurement:

While specific password content is not typically audited directly for privacy reasons, compliance with password *policies* (enforced by system settings like minimum length and complexity) and these *guidelines* (through training and awareness) will be assessed. The designated IT authority (e.g., Precision Computer team) may verify compliance through system configuration checks, security audits, monitoring for weak password usage where detectable, and user awareness programs.

5.2 Exceptions:

System-level constraints may occasionally prevent adherence to the ideal length recommendation. Any exceptions to enforced password policies require justification and approval from the designated IT authority (e.g., Precision Computer team).

5.3 Responsibility:

Users are responsible for creating passwords consistent with these guidelines and for protecting their passwords from disclosure. Violations of enforced password policies may lead to account lockout or disciplinary action.

6.0 Definitions

* **Password:** A secret string of characters used to authenticate a user to a system or service.
* **Passphrase:** A sequence of words or other text used as a password, typically longer and potentially easier to remember than complex character strings.
* **Password Manager:** Software designed to securely store and manage user passwords for various accounts.
* **Multi-Factor Authentication (MFA):** A security process requiring users to provide two or more different authentication factors to verify their identity (e.g., something they know [password], something they have [token/phone], something they are [biometric]).

7.0 Related Policies

* Password Policy (which defines mandatory requirements like minimum length, history, expiration)
* Acceptable Use Policy
* Information Security Policy (Overall)
* Remote Access Policy

Revision #2
Created 28 August 2024 16:56:13 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery