Password Protection Policy

1.0 Purpose

Passwords are a critical security control for protecting user accounts, organizational systems, and sensitive information. This policy establishes the mandatory standards for password creation, protection, management, and system-level handling to prevent unauthorized access and mitigate security risks associated with weak or compromised passwords. Adherence to this policy is essential for maintaining the security and integrity of the organization's IT environment.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and any other individuals ("Users") who have or are responsible for any account or form of access requiring a password on any system that:

* Resides within any organizational facility.
* Connects to the organization's network.
* Stores non-public organizational information.

This includes user accounts, service accounts, administrative accounts, application accounts, network device accounts, etc. It also applies to application developers designing systems that handle authentication.

3.0 Policy Statements

3.1 User Responsibilities: Password Creation and Protection

* **Mandatory Requirements:** All passwords used to access organizational resources must meet the minimum requirements enforced by the respective systems. These requirements typically include:
    * **(Placeholder: Minimum Length - e.g., 12 characters)**
    * **(Placeholder: Complexity Requirements - e.g., Must contain characters from 3 of the following 4 categories: Uppercase letters, Lowercase letters, Numbers, Symbols)**
    * **(Placeholder: Password History - e.g., Cannot reuse the last 10 passwords)**
    * **(Placeholder: Maximum Password Age - e.g., Must be changed every 90 days)**
    (Note: The specific values for the placeholders above must be defined and configured by the organization based on risk assessment and best practices).
* **Password Confidentiality:** Users must keep their passwords confidential. Passwords must not be shared with anyone, including colleagues, supervisors, family members, or IT support staff. (IT support will use other methods for assistance). Passwords must not be written down in unsecured locations (e.g., sticky notes, unsecured files).
* **Uniqueness:** Passwords must be unique to each organizational account and should not be reused across different systems or external non-organizational accounts.

*   **Suspicion of Compromise:** If a user suspects their password has been compromised, they must change it immediately and report the suspicion to the IT Help Desk or designated security contact.
*   **Guidance:** Users should follow the best practices outlined in the organization's **Password Creation Guideline** for creating strong, memorable passwords or passphrases that meet these policy requirements.

3.2 System and Application Requirements (Developer/Administrator Responsibilities)

*   **Individual Authentication:** Systems and applications must authenticate individual users. Use of shared or group accounts should be minimized and requires specific approval and controls.
*   **Secure Storage:** Passwords must **never** be stored in clear text or any easily reversible format (e.g., weak hashing, simple encryption with embedded keys). Strong, salted, adaptive hashing algorithms (e.g., bcrypt, scrypt, Argon2, PBKDF2) must be used for storing password hashes. Refer to Secure Database Credential Handling Policy for application credential storage.
*   **Secure Transmission:** Passwords must **never** be transmitted in clear text over any network. Secure, encrypted protocols (e.g., TLS/SSL, SSH) must be used for all authentication processes involving password transmission.
*   **Role Management/Delegation:** Applications should provide mechanisms for role management or delegation (e.g., impersonation, delegated authority) so that administrative tasks or functional coverage can occur without requiring users to share their personal passwords.
*   **Password Policy Enforcement:** Systems must be configured to technically enforce the mandatory password requirements defined in section 3.1 (minimum length, complexity, history, expiration).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods. These include technical enforcement checks via system configurations, audits of password storage mechanisms in applications, security assessments, review of account management procedures, internal/external audits, and analysis of authentication logs.

4.2 Exceptions

Any exception to this policy (e.g., for specific system accounts or legacy applications where requirements cannot be met) requires formal, documented justification, risk assessment identifying compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

*   Failure by users to comply with password protection requirements may result in disciplinary action, up to and including termination of employment or contract.
*   Failure by system administrators or developers to ensure systems comply with the technical

requirements of this policy may result in requirements for immediate remediation, system isolation, or disciplinary action.
* Accounts with non-compliant passwords may be disabled until brought into compliance.

5.0 Definitions

* **Password:** A secret string of characters used to authenticate a user to a system or service.
* **Password Hash:** A one-way cryptographic representation of a password, used for secure storage and comparison.
* **Salt:** Random data added to a password before hashing to make precomputed hash attacks (e.g., rainbow tables) ineffective.
* **Clear Text:** Unencrypted, human-readable data.

6.0 Related Policies and Guidelines

* Password Creation Guideline
* Acceptable Use Policy
* Information Security Policy (Overall)
* Secure Database Credential Handling Policy
* Secure Development Policy / Standards
* Remote Access Policy
* Account Management Policy

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