# Password Policy

A **password policy** is a critical component of an organization's cybersecurity framework, establishing guidelines for creating, using, and managing passwords securely. This document outlines best practices and detailed recommendations to protect systems, data, and user accounts from unauthorized access.

**1. Password Creation Standards**

**1.1 Length Requirements**

* Minimum password length: **12 characters** (14+ recommended for higher security).
* Administrative accounts: Require **16+ characters**.

**1.2 Complexity Requirements**

* Passwords must contain characters from at least **three** of the following four categories:
  1. Uppercase letters (A–Z)
  2. Lowercase letters (a–z)
  3. Numbers (0–9)
  4. Special characters (e.g., ! @ # $ % ^ & \* ?)
* Passwords must **avoid predictable patterns**, such as:
  1. Consecutive or repetitive characters (e.g., aaaaaa, 123456).
  2. Sequential patterns on keyboards (e.g., qwerty, 123qwe).
  3. Dictionary words, common phrases, or common substitutions (e.g., P@ssw0rd).
* Prohibit the use of **personal information**, such as:
  1. Names (usernames, family members, pets).
  2. Birthdates, anniversaries, or phone numbers.

**1.3 Prohibited Password Examples**

* Avoid passwords commonly found in breach databases or those flagged as weak by tools like Have I Been Pwned.

**2. Password Management Requirements**

**2.1 Password Expiration**

* Passwords should expire every **90 days** for standard accounts unless MFA is in place.
* For administrative or privileged accounts:
  + Expire passwords every **30–60 days**.

**2.2 Password History**

* Prevent reuse of the **last 5–10 passwords**.
* Maintain a password history log to enforce this rule.

**2.3 Password Strength Testing**

* Use automated tools to evaluate password strength during creation.
* Block known weak, breached, or commonly used passwords.

**2.4 Password Storage**

* Users must store passwords securely using:
  + **Password managers** approved by the organization.
  + Secure, encrypted storage solutions for team/shared passwords.
* Do **not write passwords** on paper, in plaintext files, or unencrypted formats.

**3. Authentication Enhancements**

**3.1 Multi-Factor Authentication (MFA)**

* Enforce MFA across all accounts, particularly for:
  + Administrative access.
  + Remote logins.
  + Access to sensitive data or financial systems.
* Types of MFA:
  + Mobile-based authenticator apps (e.g., Google Authenticator, Duo).
  + Hardware tokens (e.g., YubiKey).
  + Biometric verification (e.g., fingerprints, facial recognition).

**3.2 Single Sign-On (SSO)**

* Where applicable, use SSO with robust authentication protocols (e.g., SAML, OAuth) to centralize authentication while maintaining security.

**4. Account Lockout Policy**

**4.1 Failed Login Attempts**

* Lock accounts after **5–10 consecutive failed login attempts** to mitigate brute-force attacks.
* Lockout duration:
  + Temporary lockout for **15–30 minutes**, or
  + Permanent lockout requiring administrator intervention.

**4.2 Account Notifications**

* Notify users of:
  + Failed login attempts.
  + Suspicious activity on their accounts.
  + Password changes or resets.

**5. Password Sharing and Confidentiality**

**5.1 Sharing Prohibition**

* Users must **never share passwords**, even with trusted colleagues.
* Implement technical controls to prevent shared accounts.

**5.2 Awareness of Social Engineering Risks**

* Train users to recognize and avoid:
  + Phishing emails requesting credentials.
  + Phone-based social engineering (vishing).
  + Fake websites designed to harvest passwords.

**6. Password Reset and Recovery Standards**

**6.1 Identity Verification**

* Verify identity using:
  + Secondary factors such as email, SMS, or security questions (avoid weak or guessable questions).
  + MFA during the reset process.

**6.2 Temporary Passwords**

* Temporary passwords issued during recovery must:
  + Be random and meet complexity requirements.
  + Expire after **one-time use** or within a short timeframe (e.g., 24 hours).

**7. Administrative and Privileged Accounts**

**7.1 Elevated Password Standards**

* Require administrative passwords to be:
  + **Longer** (16+ characters).
  + **Unique** from standard user accounts.
* Mandate MFA for all privileged accounts.

**7.2 Password Rotation**

* Rotate administrative credentials more frequently than user credentials (e.g., every 30 days).

**7.3 Shared Administrator Accounts**

* Avoid shared administrative accounts.
* Use individual accounts with privileged access assigned as needed.

**8. Education and Awareness**

**8.1 Regular Training**

* Conduct mandatory training sessions for employees on:
  + Importance of strong, unique passwords.
  + Risks of password reuse and weak passwords.
  + Use of password managers.
  + Recognizing phishing attacks and social engineering.

**8.2 Communication of Policy Changes**

* Notify users promptly of any changes to the password policy or guidelines.

**9. Monitoring and Enforcement**

**9.1 Automated Enforcement Tools**

* Deploy automated tools to:
  + Enforce password complexity and history rules.
  + Detect and prevent the use of breached or weak passwords.
  + Monitor for unusual activity (e.g., multiple failed login attempts).

**9.2 Breach Monitoring**

* Regularly scan internal and external systems for credential leaks.
* Integrate third-party services to detect compromised passwords (e.g., Have I Been Pwned APIs).

**10. Compliance and Review**

**10.1 Periodic Review**

* Review and update the password policy annually or when new threats emerge.

**10.2 Regulatory Compliance**

* Ensure compliance with relevant regulations, such as:
  + GDPR (General Data Protection Regulation)
  + CCPA (California Consumer Privacy Act)
  + HIPAA (Health Insurance Portability and Accountability Act)
  + NIST (National Institute of Standards and Technology) SP 800-63 guidelines.

**10.3 Auditing**

* Conduct periodic audits to verify:
  + Adherence to password policies.
  + Security of password storage systems.