Password Policy

Purpose

This policy outlines password requirements for all users accessing business systems, applications, or data. It is designed to reduce risk, improve usability, and align with current best practices from the National Institute of Standards and Technology (NIST).

Scope

Applies to all employees, contractors, and third-party users with access to company-managed systems.

Password Policy

1. Password Creation

Minimum length: **8 characters**

No mandatory complexity rules (e.g., symbols or uppercase letters), though users are encouraged to use **passphrases** for better memorability

Passwords must not:

- Be common or easily guessed (e.g., “123456,” “password,” “qwerty”)
- Appear in known breach databases or dark web corpuses
- Be reused across multiple accounts or recycled from previous passwords

Systems should check new passwords against a list of known compromised credentials.

2. Password Storage and Transmission

Passwords must be stored using **secure hashing algorithms** such as bcrypt, PBKDF2, or Argon2

Passwords must be encrypted during transmission using TLS or equivalent protocols

3. Password Expiration and Rotation

Passwords should **not expire arbitrarily**

Changes are only required if there is evidence of compromise or breach

Forced rotation is discouraged unless mandated by external compliance frameworks

Password Policy

4. Account Lockout and Rate Limiting

Systems must implement rate limiting to prevent brute-force attacks

After multiple failed login attempts, accounts may be temporarily locked or require CAPTCHA

Lockout thresholds should balance security with usability

5. Multifactor Authentication (MFA)

MFA is required for access to sensitive systems and data

Acceptable second factors include:

Time-based one-time passwords (TOTP)

Hardware tokens

Biometric authentication

Push notifications via trusted apps

6. Password Managers

Users are encouraged to use approved password managers to store and generate credentials

Password managers should support encryption, breach monitoring, and secure sharing

7. Incident Response

If a password is suspected to be compromised, users must report it immediately

IT or security teams should initiate credential reset and audit access logs

Breach notifications should follow the organization's incident response protocol