Password Policy Template

Document Control Information

- **Document Title:** Password Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Password Policy establishes [ORGANIZATION NAME]'s requirements for creating, managing, and protecting passwords in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that passwords are strong, secure, and properly managed throughout their lifecycle.

1.2 Scope

This policy applies to all passwords used to access [ORGANIZATION NAME]'s information systems, applications, and services, including: - User account passwords - System and service account passwords - Application passwords - Network device passwords - Database passwords - Cloud service passwords - All employees, contractors, consultants, temporary staff, and other workers - All third parties with access to [ORGANIZATION NAME]'s systems

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing strong password requirements - Ensuring passwords are properly protected and managed - Educating users on secure password practices - Implementing additional authentication mechanisms where appropriate - Regularly reviewing and updating password requirements based on evolving threats

2. Password Creation and Complexity

2.1 Password Complexity Requirements

All passwords must meet the following minimum requirements:

2.1.1 User Passwords

- Minimum length of [12] characters
- Must contain at least one character from three of the following four categories:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special characters (e.g., !@#$%^&*()_+)
- Must not contain the user's username, employee ID, or name
- Must not contain easily guessable information (e.g., common words, organization name)
- Must not be identical to previously used passwords

2.1.2 System and Service Account Passwords

- Minimum length of [16] characters
- Must contain at least one character from all four of the following categories:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special characters (e.g., !@#$%^&*()_+)
- Must be unique for each system or service
- Must be generated using a secure random password generator where possible

2.1.3 Application Default Passwords

- Default or initial passwords must be unique for each installation
- Must meet the same complexity requirements as system passwords
- Must be changed immediately after installation or initial use

2.2 Password Generation

- Users are encouraged to use passphrases (multiple words combined with numbers and special characters)
- Password managers may be used to generate and store complex passwords
- Random password generators should be used for system and service accounts

2.3 Prohibited Password Practices

The following practices are prohibited: - Using common or easily guessable passwords - Using the same password for multiple systems or accounts - Using personal information in passwords - Sharing passwords with others - Writing down passwords in unsecured locations - Using sequential or repeated characters (e.g., 12345, aaaaa) - Using organization name or commonly used terms

3. Password Management

3.1 Password Expiration and Changes

3.1.1 User Passwords

- Passwords shall expire after [90] days
- Users shall be notified [14] days before password expiration
- Users shall not reuse the previous [12] passwords
- Users shall not change passwords more than once per day

3.1.2 System and Service Account Passwords

- Passwords shall expire after [180] days
- System administrators shall be notified [30] days before expiration
- Passwords shall not be reused
- Password changes shall be coordinated to minimize service disruption

3.2 Initial Password Assignment

- Initial passwords shall be set to unique, temporary values
- Initial passwords shall be communicated securely to users
- Users shall be required to change initial passwords at first login
- Initial passwords shall expire after [24] hours if not used

3.3 Password Reset Procedures

- Users must verify their identity before password resets
- Temporary passwords must meet complexity requirements
- Temporary passwords must expire after [24] hours
- Users must change temporary passwords at first login
- Password resets must be logged and monitored

3.4 Password Storage and Transmission

- Passwords must never be stored in clear text

- Passwords must be stored using strong, industry-standard hashing algorithms
- Password hashes must be salted with unique, random values
- Passwords must never be transmitted in clear text
- Secure protocols must be used when passwords are transmitted

4. Authentication Controls

4.1 Account Lockout

- Accounts shall be locked after [5] consecutive failed login attempts
- Locked accounts shall remain locked for [30] minutes or until unlocked by an administrator
- Failed login attempts shall be logged and monitored
- Users shall be notified when their account is locked

4.2 Multi-Factor Authentication (MFA)

- MFA shall be implemented for:
  - Remote access to the network
  - Access to privileged accounts
  - Access to sensitive systems and data
  - Access to cloud services
  - [OTHER SYSTEMS AS APPROPRIATE]
- MFA methods may include:
  - Mobile authenticator apps
  - Hardware tokens
  - SMS or email one-time passwords (least preferred)
  - Biometric authentication
  - Smart cards

4.3 Session Management

- User sessions shall automatically lock after [15] minutes of inactivity
- Users shall be required to re-authenticate after session timeout
- Users shall be able to manually lock their sessions when leaving their workstation
- Concurrent sessions may be limited based on risk assessment

5. Special Account Types

5.1 Privileged Accounts

- Privileged accounts shall have stronger password requirements

- Privileged account passwords shall be changed more frequently
- Privileged accounts shall always require MFA
- Use of privileged accounts shall be logged and monitored
- Privileged accounts shall only be used for administrative tasks

5.2 Shared Accounts

- Shared accounts shall be avoided whenever possible
- When necessary, shared accounts shall:
    - Be approved by management
    - Have a designated owner
    - Have passwords changed when a user with knowledge of the password leaves
    - Have passwords changed regularly
    - Have usage logged and monitored

5.3 Emergency Access Accounts

- Emergency access accounts shall be established for critical systems
- Emergency access passwords shall be:
    - Highly complex
    - Stored securely with restricted access
    - Changed after each use
    - Regularly tested
    - Logged when used

6. Password Protection

6.1 User Responsibilities

Users are responsible for: - Keeping passwords confidential - Not sharing passwords with anyone, including IT staff - Not storing passwords in unsecured locations - Reporting suspected password compromises immediately - Complying with all password requirements

6.2 Administrator Responsibilities

Administrators are responsible for: - Implementing technical controls to enforce this policy - Assisting users with password issues - Not requesting user passwords - Ensuring system passwords are properly secured - Regularly reviewing password compliance

6.3 Password Manager Use

- [ORGANIZATION NAME] [encourages/requires] the use of approved password managers
- Password managers must be approved by the Information Security team
- The master password for password managers must be strong and memorable
- Password managers should be used to generate and store complex passwords
- Password manager data must be backed up securely

7. Compliance and Exceptions

7.1 Compliance Monitoring

- Technical controls shall be implemented to enforce password requirements
- Regular audits shall verify compliance with this policy
- Password strength shall be evaluated during security assessments
- Password-related security incidents shall be investigated

7.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

8. Related Documents

- Information Security Policy
- Access Control Policy
- Multi-Factor Authentication Procedure
- Account Management Procedure
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

9. Approval

This Password Policy is approved by:

Name: _______________________ Position: _____________________ Date: ________________________ Signature: ____________________