Password Security Policy

[Your Company Name]

Document ID: PS-POL-001

Effective Date: [Date]

Last Updated: [Date]

Version: 1.0

Author: [Your Name]

Table of Contents

1. Introduction

1.1 Purpose

This Password Security Policy is established to ensure that [Your Company Name] employees and authorized users adhere to secure password practices. It aims to protect sensitive information and systems from unauthorized access or breaches.

1.2 Scope

This policy applies to all users who have access to [Your Company Name] systems, networks, and resources.

1.3 Policy Objectives

- Establish guidelines for creating strong and secure passwords.
- Define the frequency of password changes.
- Ensure safe storage and transmission of passwords.

- Clarify user responsibilities and consequences of non-compliance.

2. Password Creation and Complexity

2.1 Password Requirements

- Passwords must be at least [number] characters long.
- Passwords must contain a combination of uppercase and lowercase letters, numbers, and special characters.
- Passwords should not contain easily guessable information (e.g., names, birthdays).
- Passwords must be unique and not reused within [number] previous passwords.

2.2 Password Change Frequency

- Users are required to change their passwords every [number] days.
- Exceptions may apply for specific user groups, subject to approval from the IT department.

2.3 Password Expiration

- Passwords will expire after [number] days.
- Users will receive automated notifications [number] days before password expiration.

3. Password Storage

3.1 Password Storage Practices

- Passwords must never be written down or stored in unsecured locations.
- Digital password storage must be encrypted and protected with strong access controls.

3.2 Password Sharing

- Passwords must never be shared with others, including colleagues or IT personnel.
- Shared or temporary accounts must be approved by the IT department.

4. Password Transmission and Encryption

4.1 Secure Transmission

- Passwords must not be transmitted over insecure channels (e.g., plain text emails).
- When transmitting passwords, use secure methods such as encrypted communication protocols.

4.2 Encryption of Stored Passwords

- All stored passwords must be hashed and salted to protect against data breaches.

5. User Responsibilities

5.1 Account Ownership

- Users are responsible for all actions taken using their accounts.
- Sharing of accounts or allowing others to use their credentials is strictly prohibited.

5.2 Password Sharing

- Users should never request or share passwords with anyone, even IT personnel, without proper authentication.

5.3 Reporting Suspicious Activity

- Users are encouraged to report any suspicious password-related activity to the IT department.

6. Password Management

6.1 Password Reset Procedures

- Users who forget their passwords should follow the established password reset procedures.

- Password reset requests may be subject to identity verification.

6.2 Forgotten Passwords

- Users must contact the IT department for assistance in case of forgotten passwords.

7. Enforcement and Compliance

7.1 Auditing and Monitoring

- [Your Company Name] will regularly audit and monitor password usage and compliance.
- Non-compliance may result in disciplinary action, up to and including account suspension.

7.2 Non-Compliance

- Failure to adhere to this policy may lead to loss of access, disciplinary action, and potential legal consequences.

8. Review and Revision

This Password Security Policy will be reviewed annually and updated as necessary to align with best practices and [Your Company Name]'s evolving security needs.

Approval:

This policy is approved by:

[Your Name]

[Your Title]

[Date]