Password Management Policy Sample

1. Purpose

The purpose of this Password Management Policy is to establish minimum standards for the creation, maintenance, and protection of passwords used to access **[Company]** information systems and resources.

2. Scope

This policy applies to all employees, contractors, and third-party users who have access to **[Company]** systems or data.

3. Policy

3.1 Password Creation

- Passwords must be at least 12 characters in length.
- Passwords must contain a mix of uppercase and lowercase letters, numbers, and special characters.
- Passwords must not contain easily guessed information such as names, usernames, or birthdays.

3.2 Password Management

- Passwords must be changed every 90 days.
- Passwords must not be reused within a 6-password history.
- Unique passwords must be used for different accounts.

3.3 Password Protection

- Passwords must not be shared with anyone.
- Passwords must not be written down or stored in plaintext.
- Password management tools approved by **[Company]** may be used.

3.4 System Requirements

- Systems must enforce password requirements outlined in this policy.
- Accounts will be locked after 5 unsuccessful login attempts.
- Multi-factor authentication (MFA) must be used where applicable.

4. Enforcement

Violation of this policy may result in disciplinary action up to and including termination of employment or contract.

5. Review

This policy will be reviewed annually or as needed to address new security threats or changes in technology.

6. Contact

For questions about this policy, contact the IT Department at *[contact email/phone]*.