Example Password Policy

This is an example password policy. Use this as a guide to write or revise the password policy for your organization.

~~~~~~~

Password Policy

1.0 Purpose

The purpose of this policy is to protect the organization's information assets by ensuring the creation, management, and maintenance of secure passwords and to ensure compliance with relevant laws and regulations.

2.0 Scope

This policy applies to all employees, contractors, and third-party vendors who have access to organizational information systems and data.

3.0 Policy

3.1 All passwords must meet the complexity requirements defined by the IT department. These requirements include a minimum length of 12 characters and the use of at least one uppercase letter, one lowercase letter, one number, and one special character. Passwords should not contain easily guessable information, such as the user's name or username or common words.

3.2 Passwords must be changed every 90 days.

3.3 Passwords must not be shared or written down in an easily accessible location. Passwords should be stored securely using password management tools to ensure they are protected from unauthorized access.

3.4 Multifactor authentication (MFA) is required for accessing sensitive systems and data.

3.5 Accounts must be locked after five unsuccessful login attempts and can only be unlocked by the IT department or automatically unlocked after a specified duration (for example, 30 minutes).

3.6 Users who suspect that their password has been compromised must change it immediately and notify the IT department.

3.7 All users must undergo regular training on password security best practices and the importance of adhering to the password policy.

4.0 Responsibilities

Employees

- Follow password creation and management protocols and report any suspected security incidents immediately

IT Department

- Implement and enforce password complexity requirements, monitor compliance, and provide support for password resets and account unlocks

Managers

- Ensure their teams adhere to the password policy and support the IT department in enforcing the policy

Security Officer

- Oversee the password security strategy, ensure policy enforcement, and conduct regular audits

5.0 Compliance

Compliance with this policy is mandatory for all employees, contractors, and stakeholders. Noncompliance may result in disciplinary actions, including termination of employment, and could lead to legal consequences if it involves violations of laws and regulations.

6.0 Enforcement

This policy will be enforced with regular audits and continuous monitoring conducted by the security officer. Any violations of the policy will be subject to thorough investigation, and appropriate disciplinary measures will be taken based on the severity of the noncompliance. Actions may include warnings, retraining, suspension, or termination, depending on the nature of the violation.

7.0 Definitions

- **Password complexity requirements:** specifications for creating a secure password, including minimum length and use of upper- and lowercase letters, numbers, and special characters
- **Multifactor authentication (MFA):** an authentication method that requires more than one piece of evidence to verify the user's identity

8.0 Review and Updates

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. The security officer is responsible for coordinating the review and update process. A revision history will be maintained to document changes and updates.

Revision History

Date	Description of Change	Changed By
YYYY-MM-DD	[Initial draft or specific changes made]	[Name or role]