Password Policy

---

1. Purpose

The purpose of this Password Policy is to establish guidelines for creating, managing, and protecting passwords to ensure the security of [Organization Name]'s systems, data, and resources.

---

2. Scope

This policy applies to all employees, contractors, interns, and third parties who access [Organization Name]'s systems or networks. It covers all accounts, including but not limited to email, network, and application accounts.

---

3. Password Creation

- **Length**: Passwords must be at least 12 characters long.
- **Complexity**: Passwords must include a mix of:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Numbers (0-9)
    - Special characters (e.g., !, @, #, $)
- **Uniqueness**: Passwords must be unique and not reused across different accounts.

---

4. Password Management

- **Password Changes**: Passwords must be changed every 90 days.
- **Password History**: Users cannot reuse their last 5 passwords.
- **Password Sharing**: Passwords must not be shared with anyone, including colleagues or IT staff.
- **Password Storage**: Passwords must not be written down or stored in unsecured locations (e.g., sticky notes, unencrypted files).

---

5. Multi-Factor Authentication (MFA)

- **Requirement**: MFA must be enabled for all accounts that support it.
- **Methods**: Use one of the following for MFA:
    - Authentication apps (e.g., Google Authenticator, Microsoft Authenticator)
    - SMS-based codes
    - Hardware tokens

---

6. Account Lockout

- **Failed Attempts**: Accounts will be locked after 5 failed login attempts.
- **Lockout Duration**: Accounts will remain locked for 30 minutes or until unlocked by an administrator.

---

7. Password Recovery

- **Self-Service**: Users can reset their passwords using the self-service password reset tool.
- **IT Assistance**: If self-service is unavailable, users must contact the IT department for assistance.
- **Identity Verification**: Users must verify their identity before a password reset is performed.

---

8. Enforcement

- **Monitoring**: The IT department will monitor password compliance and enforce this policy.
- **Violations**: Violations of this policy may result in disciplinary action, up to and including termination of employment.

---

9. Acknowledgment

All users must acknowledge that they have read, understood, and agree to comply with this Password Policy. Failure to comply may result in disciplinary action.

---

10. Review and Updates

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. Updates will be communicated to all users.

Acknowledgment Form

I, [Full Name], acknowledge that I have read, understood, and agree to comply with [Organization Name]'s Password Policy. I understand that violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.
Signature: _____
Date: _____

How to Use This Password Policy

1. **Customize**: Replace placeholders like `[Organization Name]` with your organization's details.
2. **Distribute**: Share the Password Policy with all employees and require them to sign the acknowledgment form.
3. **Enforce**: Ensure compliance by monitoring password practices and addressing violations promptly.