Prompt: Generate a policy for password policy.

**Password Policy**

**1. Purpose**

The purpose of this policy is to establish standards for creating strong passwords, protecting those passwords, and the frequency of changing them.

**2. Scope**

This policy applies to all employees, contractors, and third-party users who have access to [Organization Name] information systems and data.

**3. Password Creation Standards**

* **Password Length**: Passwords must be at least 12 characters long.
* **Password Complexity**: Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters.
* **Avoid Common Words**: Passwords should not include common words, phrases, or predictable sequences.
* **Personal Information**: Passwords must not contain personal information such as names, birthdays, or addresses.

**4. Password Protection Standards**

* **Password Confidentiality**: Passwords should not be shared with anyone, including supervisors or IT staff.
* **Password Storage**: Passwords must not be written down or stored in an unencrypted format.
* **Password Transmission**: Passwords should never be transmitted via email, chat, or other unsecured communication methods.

**5. Password Expiration and Change Management**

* **Password Expiration**: Passwords must be changed every 90 days.
* **Password History**: Users cannot reuse any of their last 12 passwords.
* **Password Change for Compromised Accounts**: If a password is suspected to be compromised, it must be changed immediately.

**6. Account Lockout**

* **Failed Attempts**: Accounts will be locked out after 5 failed login attempts.
* **Lockout Duration**: Locked accounts will remain locked for a minimum of 30 minutes or until manually unlocked by an administrator.

**7. Multi-Factor Authentication (MFA)**

* **MFA Requirement**: MFA is required for accessing sensitive systems and data.
* **MFA Methods**: Approved MFA methods include SMS codes, authenticator apps, and hardware tokens.

**8. Training and Awareness**

* **Regular Training**: Employees must undergo regular training on password security best practices.
* **Awareness Programs**: The organization will conduct periodic awareness programs to educate employees about the importance of password security.

**9. Compliance**

* **Policy Adherence**: All users are responsible for adhering to this password policy.
* **Audits**: Regular audits will be conducted to ensure compliance with this policy.
* **Non-Compliance**: Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or access.

**10. Review and Revision**

* **Policy Review**: This policy will be reviewed annually and updated as necessary to address new security threats and best practices.
* **Feedback**: Employees are encouraged to provide feedback on this policy to help improve its effectiveness.

**Implementation**

This policy will be communicated to all employees and relevant stakeholders. Training sessions will be organized to ensure everyone understands the requirements and their responsibilities under this policy.

**Contact Information**

For questions or concerns regarding this password policy, please contact the IT Security Department at [contact information].