Prompt: Generate a policy for password policy.

**Corporate Password Policy**

**1. Purpose and Scope**

This password policy establishes minimum requirements for creating, managing, and protecting passwords across all organizational systems and accounts. This policy applies to all employees, contractors, vendors, and any individual with access to organizational information systems.

**2. Password Requirements**

**2.1 Complexity Standards**

All passwords must meet the following minimum criteria:

* **Minimum Length**: 12 characters for standard accounts, 16 characters for administrative accounts
* **Character Composition**: Must include at least three of the following four character types:
  + Uppercase letters (A-Z)
  + Lowercase letters (a-z)
  + Numbers (0-9)
  + Special characters (!@#$%^&\*()\_+-=[]{}|;:,.<>?)
* **No Dictionary Words**: Passwords should not contain complete dictionary words or common phrases
* **No Personal Information**: Passwords must not contain personal information such as names, birthdates, addresses, or phone numbers

**2.2 Prohibited Passwords**

The following are strictly prohibited:

* Previously used passwords (last 12 passwords)
* Default or vendor-supplied passwords
* Passwords shared among multiple accounts
* Common passwords (e.g., "password123", "admin", "welcome")
* Sequential characters (e.g., "123456", "abcdef")
* Repeated characters (e.g., "aaaaaa", "111111")

**3. Password Management**

**3.1 Password Creation Guidelines**

* Use passphrases when possible (e.g., "Coffee!Morning$Run#Daily2024")
* Consider using the first letters of a memorable sentence with numbers and symbols
* Utilize approved password managers for generating and storing complex passwords
* Never write passwords down in plaintext or store them in unsecured locations

**3.2 Password Storage**

* All passwords must be stored using approved password management solutions
* Personal password managers must be approved by IT security team
* Shared account passwords must be stored in enterprise password management systems
* Browser-saved passwords are discouraged for business accounts

**3.3 Password Expiration and Rotation**

* **Standard User Accounts**: Passwords expire every 90 days
* **Administrative Accounts**: Passwords expire every 60 days
* **Service Accounts**: Passwords expire annually or as determined by risk assessment
* **Shared Accounts**: Passwords must be changed immediately when personnel with access leave the organization

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

**4.1 MFA Requirements**

Multi-factor authentication is required for:

* All administrative accounts
* Remote access to corporate networks
* Access to sensitive data systems
* Cloud-based business applications
* Email systems

**4.2 Approved MFA Methods**

* Hardware security keys (preferred)
* Mobile authenticator applications
* SMS verification (as backup only)
* Biometric authentication where supported

**5. Account Security Measures**

**5.1 Account Lockout Policy**

* Accounts will be locked after 5 consecutive failed login attempts
* Lockout duration: 30 minutes for standard accounts, 60 minutes for administrative accounts
* Manual unlock required for repeated lockout events

**5.2 Password Reset Procedures**

* Self-service password reset available through approved identity management systems
* Help desk verification required for password resets involving:
  + Administrative accounts
  + Multiple recent reset requests
  + Suspicious circumstances
* Identity verification required before password reset assistance

**6. Roles and Responsibilities**

**6.1 Users**

* Create strong passwords according to policy requirements
* Protect passwords from unauthorized disclosure
* Report suspected password compromise immediately
* Use approved password management tools
* Complete required security awareness training

**6.2 IT Security Team**

* Monitor password policy compliance
* Maintain approved password management solutions
* Investigate password-related security incidents
* Provide security awareness training
* Regular policy review and updates

**6.3 System Administrators**

* Implement technical controls to enforce password policies
* Configure systems to require compliant passwords
* Monitor for policy violations
* Maintain audit logs of password-related activities

**7. Incident Response**

**7.1 Suspected Compromise**

If a password is suspected to be compromised:

1. **Immediate Action**: Change the password immediately
2. **Notification**: Report the incident to IT Security within 2 hours
3. **Assessment**: Review account activity for unauthorized access
4. **Documentation**: Complete incident report form
5. **Follow-up**: Implement additional security measures as recommended

**7.2 Breach Response**

In case of confirmed password breach:

* Immediate password reset for affected accounts
* Review of access logs and system activities
* Assessment of data exposure risk
* Implementation of additional monitoring
* Notification to relevant stakeholders per incident response plan

**8. Compliance and Monitoring**

**8.1 Regular Audits**

* Quarterly password policy compliance assessments
* Annual penetration testing including password attacks
* Monthly reports on password policy violations
* Regular review of password management tool effectiveness

**8.2 Policy Violations**

Violations of this password policy may result in:

* Mandatory security awareness training
* Temporary account suspension
* Disciplinary action per HR policies
* Revocation of system access privileges

**9. Exceptions and Approvals**

**9.1 Exception Process**

Exceptions to this policy require:

* Written business justification
* Risk assessment and mitigation plan
* Approval from IT Security Manager and department head
* Regular review of approved exceptions
* Documentation of compensating controls

**9.2 Legacy Systems**

For systems unable to support full policy requirements:

* Document technical limitations
* Implement maximum possible security controls
* Establish compensating security measures
* Plan for system upgrades or replacement
* Increased monitoring and access restrictions

**10. Training and Awareness**

**10.1 Required Training**

All personnel must complete:

* Initial password security training within 30 days of access
* Annual refresher training
* Specialized training for administrative account holders
* Additional training following security incidents

**10.2 Awareness Program**

Ongoing security awareness includes:

* Monthly security tips and reminders
* Simulated phishing exercises
* Password security best practices communication
* Recognition of social engineering attempts

**11. Policy Review and Updates**

This password policy will be reviewed annually or following significant security incidents. Updates will be communicated to all affected personnel with appropriate training provided for policy changes.

**Effective Date**: [Insert Date]  
**Next Review Date**: [Insert Date]  
**Policy Owner**: IT Security Manager  
**Approved By**: [Insert Name and Title]