Prompt: Generate a Secure password policy. Ensure security best practices.   
  
**Password Policy**

Generate a policy for password policy. Ensure security best practices.

**Enterprise Password Security Policy**

**1. Purpose and Scope**

This policy establishes mandatory requirements for password creation, management, and security across all organizational systems, applications, and accounts. It applies to all employees, contractors, vendors, and third parties with access to company systems.

**2. Password Requirements**

**2.1 Minimum Standards**

* **Length**: Minimum 12 characters, recommended 16+ characters
* **Complexity**: Must include at least three of the following:
  + Uppercase letters (A-Z)
  + Lowercase letters (a-z)
  + Numbers (0-9)
  + Special characters (!@#$%^&\*()\_+-=[]{}|;:,.<>?)
* **Uniqueness**: Cannot reuse the last 12 passwords
* **Dictionary Check**: Cannot contain common dictionary words or predictable patterns

**2.2 Prohibited Passwords**

* Personal information (names, birthdays, addresses, phone numbers)
* Company information (organization name, departments, common terms)
* Sequential characters (123456, abcdef, qwerty)
* Repeated characters (aaaaaa, 111111)
* Common passwords from breach databases
* Passwords that match the username or email address

**3. Password Management**

**3.1 Password Creation**

* Use approved enterprise password managers for generation and storage
* Generate unique passwords for each system and account
* Avoid creating passwords based on personal information or patterns
* Test password strength using approved tools before implementation

**3.2 Password Storage**

* **Mandatory**: Use enterprise-approved password management solutions
* **Prohibited**: Store passwords in browsers, plain text files, spreadsheets, or sticky notes
* **Encryption**: All stored passwords must be encrypted using AES-256 or equivalent
* **Access Control**: Password vaults must require multi-factor authentication

**3.3 Password Sharing**

* **Prohibited**: Sharing personal account passwords under any circumstances
* **Service Accounts**: Shared service account passwords must be managed through approved enterprise vaults
* **Emergency Access**: Use break-glass procedures with full audit logging
* **Temporary Access**: Use time-limited, single-use passwords when necessary

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

**4.1 Mandatory Implementation**

* Required for all administrative accounts
* Required for remote access to corporate networks
* Required for access to sensitive systems and data
* Required for cloud services and SaaS applications

**4.2 Approved MFA Methods (in order of preference)**

1. Hardware security keys (FIDO2/WebAuthn)
2. Mobile authenticator apps (TOTP/HOTP)
3. SMS/Voice (only when other methods unavailable)
4. Email-based verification (least preferred)

**5. Password Lifecycle Management**

**5.1 Expiration and Rotation**

* **Administrative Accounts**: Change every 90 days
* **Service Accounts**: Change every 180 days or upon personnel changes
* **User Accounts**: No mandatory expiration if strong passwords and MFA are used
* **Compromised Passwords**: Change immediately upon suspected compromise

**5.2 Account Lockout Protection**

* Implement progressive delays after failed attempts
* Lock accounts after 5 consecutive failed attempts
* Require administrator intervention for unlock after 3 lockouts
* Monitor and alert on unusual authentication patterns

**6. Special Account Types**

**6.1 Administrative Accounts**

* Minimum 16-character passwords
* Mandatory MFA with hardware tokens
* Separate from standard user accounts
* Regular access review and certification
* Enhanced monitoring and logging

**6.2 Service Accounts**

* Minimum 20-character randomly generated passwords
* Stored in enterprise password vaults
* Regular rotation based on risk assessment
* Documented ownership and purpose
* Automated where possible to eliminate human access

**6.3 Emergency Accounts**

* Break-glass access procedures
* Time-limited activation
* Full audit logging required
* Immediate review after use
* Separate approval process for activation

**7. Implementation Guidelines**

**7.1 Technical Controls**

* Deploy enterprise password management solutions
* Implement password complexity validation in all systems
* Configure account lockout policies consistently
* Enable password history enforcement
* Deploy MFA across all applicable systems

**7.2 Monitoring and Compliance**

* Regular password audits using approved tools
* Monitor for passwords in breach databases
* Track MFA adoption and compliance rates
* Regular penetration testing of authentication systems
* Quarterly policy compliance assessments

**8. User Education and Training**

**8.1 Initial Training**

* Password security awareness during onboarding
* Hands-on training with enterprise password managers
* MFA setup and usage training
* Incident reporting procedures

**8.2 Ongoing Education**

* Annual password security refresher training
* Simulated phishing exercises
* Security awareness communications
* Regular updates on emerging threats

**9. Incident Response**

**9.1 Suspected Compromise**

* Immediately change affected passwords
* Review account activity and access logs
* Assess scope of potential data exposure
* Document incident and lessons learned
* Update security controls as needed

**9.2 Breach Response**

* Activate incident response team
* Force password resets for affected systems
* Enhance monitoring on compromised accounts
* External notification per regulatory requirements
* Post-incident security improvements

**10. Compliance and Enforcement**

**10.1 Policy Violations**

* First violation: Mandatory retraining
* Repeated violations: Progressive disciplinary action
* Severe violations: Immediate access suspension
* Document all violations and remediation actions

**10.2 Regular Reviews**

* Annual policy review and updates
* Quarterly compliance assessments
* Monthly security metrics reporting
* Continuous improvement based on threat landscape

**11. Exceptions and Approvals**

**11.1 Exception Process**

* Written business justification required
* Risk assessment and mitigation plan
* CISO or designee approval required
* Time-limited with regular review
* Enhanced monitoring for approved exceptions

**11.2 Legacy System Considerations**

* Document technical limitations
* Implement compensating controls
* Prioritize system upgrades or replacements
* Regular risk assessments
* Enhanced monitoring and access controls

**12. Policy Maintenance**

**Effective Date**: [Insert Date]  
**Review Frequency**: Annual  
**Policy Owner**: Chief Information Security Officer  
**Approval Authority**: Chief Information Officer  
**Next Review Date**: [Insert Date + 1 Year]