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

**1. Password Complexity Requirements**

* **Length**: Passwords must be at least 12 characters long.
* **Complexity**: Passwords must include a mix of uppercase letters, lowercase letters, numbers, and special characters.
* **Avoid Common Words**: Passwords should not include common words, phrases, or easily guessable information such as names or birthdays.

**2. Password Expiration and Rotation**

* **Expiration**: Passwords must be changed every 90 days.
* **History**: Users cannot reuse any of their last 12 passwords.

**3. Account Lockout**

* **Attempts**: Accounts will be locked after 5 unsuccessful login attempts.
* **Duration**: Locked accounts will remain locked for 30 minutes or until manually unlocked by an administrator.

**4. Password Storage**

* **Encryption**: Passwords must be stored using strong, industry-standard encryption algorithms (e.g., bcrypt, Argon2).
* **Access**: Access to password databases should be restricted to authorized personnel only.

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

* **Requirement**: MFA is required for all user accounts, especially for accessing sensitive information or administrative functions.
* **Methods**: Acceptable MFA methods include SMS codes, authenticator apps, hardware tokens, or biometric verification.

**6. User Education and Awareness**

* **Training**: Regular training sessions should be conducted to educate users on the importance of strong passwords and how to create them.
* **Phishing Awareness**: Users should be trained to recognize phishing attempts and other social engineering attacks.

**7. Monitoring and Auditing**

* **Logging**: All login attempts and password changes should be logged.
* **Audits**: Regular audits should be conducted to ensure compliance with the password policy and to identify any potential security issues.

**8. Password Managers**

* **Encouragement**: Users are encouraged to use reputable password managers to generate and store complex passwords securely.

**9. Administrative Controls**

* **Privileged Accounts**: Administrative or privileged accounts should have additional security measures, such as more frequent password changes and stricter complexity requirements.
* **Access Reviews**: Regular reviews of user access rights should be conducted to ensure that users have the appropriate level of access.

**10. Incident Response**

* **Breach Protocol**: In the event of a suspected password breach, immediate action should be taken to reset affected passwords and investigate the incident.
* **Notification**: Users should be promptly notified of any security incidents that may affect their accounts.

**Implementation and Enforcement**

* **Policy Distribution**: This policy should be distributed to all users and made readily available for reference.
* **Compliance**: Compliance with this policy is mandatory for all users. Non-compliance may result in disciplinary action.

By implementing this password policy, organizations can significantly enhance their security posture and protect against unauthorized access and data breaches.