PASSWORD POLICY

Password policies are critical for maintaining the security of an organization's data and systems. A good password policy helps prevent unauthorized access and protects sensitive information. Here are some important elements of password policies that organizations should follow:

Password Length

Minimum Length Requirement: Passwords should be a minimum of 8-12 characters to ensure they are not easily guessable. Longer passwords provide better security.

Complexity Requirements

Character Variety: Passwords should include a mix of upper and lower case letters, numbers, and special characters (e.g., @, #, $).

Avoid Common Words: Passwords should not contain easily guessable information like common words, user names, or company names.

Password Expiration

Regular Changes: Require users to change their passwords every 60-90 days to minimize the risk of compromised credentials.

No Reuse of Recent Passwords: Implement a policy that prevents the reuse of recent passwords (e.g., the last 5 passwords).

Account Lockout

Failed Login Attempts: After a certain number of failed login attempts (e.g., 3-5), the account should be temporarily locked to prevent brute-force attacks.

Account Recovery Procedures: Establish secure methods for account recovery if a user is locked out.

Two-Factor Authentication (2FA)

Additional Security Layer: Require 2FA where possible, combining something the user knows (password) with something the user has (e.g., a mobile device) to enhance security.

Password Storage

Encryption and Hashing: Ensure passwords are stored securely using encryption and hashing algorithms like bcrypt, which are resistant to attacks.

No Plain Text Storage: Passwords should never be stored in plain text.

User Education

Security Awareness: Educate employees about the importance of strong passwords and the risks associated with weak passwords.

Phishing Awareness: Train users on how to recognize phishing attempts that aim to steal passwords.

Enforcement and Monitoring

Automated Compliance: Use automated tools to enforce password policies across all systems.

Regular Audits: Conduct regular audits to ensure compliance with the password policy and to identify any potential vulnerabilities.

Password Sharing

Prohibition on Sharing: Explicitly forbid password sharing among employees to maintain individual accountability and security.

Role-Based Access Control (RBAC): Implement RBAC to limit access to systems based on a user's role in the organization.

Password Reset Procedures

Identity Verification: Ensure that identity verification procedures are in place before allowing a password reset.

Temporary Passwords: If a temporary password is issued during a reset, require the user to change it upon first login.