Password Management Procedure

A password management procedure provides guidance on creating and using passwords in ways that help maximize security of the password and minimize theft of the password. Passwords are the most frequently used form of authentication for accessing a computing resource

1. Password Creation Guidelines:

-Passwords should be at least 12 characters long.
-Passwords should include a combination of uppercase and lowercase letters, numbers, and special characters.
-Passwords should not be easily guessable or related to personal information.
-Passwords should be unique and not reused across different accounts.

2. Password Storage:

-Passwords should never be stored in plain text.
-Use a secure password management tool, such as LastPass or KeePass, to store and organize passwords.
-Encrypt the password management tool with a strong master password.
-Enable two-factor authentication (2FA) for the password management tool, if available.

3. Access Control:

-Grant access to password management tools only to authorized personnel who need it for their roles.
-Implement role-based access control (RBAC) to ensure appropriate access levels.
-Regularly review and update access permissions based on employee roles and responsibilities.
-Revoke access promptly for employees who leave the organization or change roles.

4. Password Sharing:

-Discourage sharing passwords via email, instant messaging, or other insecure channels. Instead
-Use a secure password sharing feature within the password management tool.
If sharing passwords with colleagues, use the tool's sharing capabilities to grant temporary access.

5. Password Change Policy:

-Enforce regular password changes, such as every 90 days.
-Notify employees in advance of upcoming password changes to avoid sudden lockouts.
-Educate employees on the importance of choosing unique and strong passwords.

6. Employee Training and Awareness:

-Conduct regular cybersecurity awareness training sessions for all employees.

-Train employees on password best practices, such as creating strong passwords and recognizing phishing attempts.
-Encourage employees to report any suspicious activities or potential security breaches.

7. Monitoring and Auditing:

-Monitor user activity within the password management tool for any unauthorized access attempts.
-Regularly audit the password management system to ensure compliance with established procedures.
-Implement alerts or notifications for any unusual or suspicious password-related activities.

Password Policy

A password policy is a set of rules and guidelines for the creation, usage, and management of passwords for its information systems and accounts. It serves as a framework to make sure that passwords are secure, protected, and are being used appropriately by employees and any other users within the organization.

1. Password Complexity:

-Passwords have to be a minimum of 12 characters long.
-Passwords have to contain a combination of uppercase and lowercase letters, numbers, and special characters.
-Avoid using common words, dictionary terms, or easily guessable information.
-Prohibit the use of sequential or repetitive characters (e.g., "12345678" or "aaaaaa").

2. Password Protection:

-Employees should never share passwords with anyone, including coworkers, supervisors, or IT staff.
-Each employee should have a unique password for their accounts.
-Avoid writing down passwords. If written down, they should be stored securely and not easily accessible.

3. Password Change and Expiration:

-Regularly change passwords, at least every 90 days.
-Passwords should not be reused for at least five previous password changes.
-Promptly change passwords if there is a suspicion of compromise or if an employee leaves the organization.
-Notify employees in advance of upcoming password changes to avoid sudden lockouts.

4. Account Lockout and Failed Login Attempts:

-Implement an account lockout policy that locks an account after a certain number of failed login attempts
-Lockout duration should be at least 15 minutes or until an administrator unlocks the account.
-Notify employees when their account has been locked due to failed login attempts.

5. Password Management and Storage:

-Encourage employees to use a secure password management tool, such as LastPass or KeePass, to store and generate strong passwords.
-Prohibit the storage of passwords in plain text or unencrypted files.
-Store passwords in an encrypted format using industry-standard encryption algorithms.

6. Two-Factor Authentication (2FA):

-Enable two-factor authentication for all accounts whenever possible.
-Encourage employees to use 2FA for their personal email accounts and other external services.

7. Employee Training and Awareness:

-Conduct regular training sessions on password security best practices.
-Educate employees on the risks of using weak passwords as well as the importance of maintaining strong, unique passwords.
-Provide guidance on recognizing and reporting phishing attempts and other suspicious activities.

8. Policy Enforcement and Consequences:

-Regularly monitor password compliance and enforce the password policy consistently.
-Apply consequences for employees who violate the policy, which may include temporary account suspension or other disciplinary actions.