SecOps® Solution

Password Protection Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

1. Overview

A crucial component of computer security is passwords. Unauthorized access to our most sensitive data and/or resource exploitation can be caused by a weak or compromised password. All employees, including contractors and vendors having access to **<Company Name>** systems, are in charge of choosing and protecting their passwords in accordance with the instructions specified below.

2. Purpose

This policy's objective is to set a standard for the safe handling and security of all passwords related to the workplace.

3. Scope

All employees who have or are in charge of an account on a system that is housed at any **<Company Name>** facility have access to the **<Company Name>** network or has any non-public **<Company Name>** information covered by this policy.

4. Policy

4.1 Password Creation and Use

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.3 Staff are allowed to use authorized, approved password managers to securely store and manage all their work related passwords.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level

privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

4.2 Password Change

4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet our Password Creation Requirements. We do not recommend the use or setting of regular password expiration.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential **<Company Name>** information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in password managers authorized by the organization.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any individual suspecting that their password may have been compromised must report the incident and change all relevant passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support the authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Multi-Factor Authentication

4.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work-related accounts but personal accounts also

5. Policy Compliance

5.1 Compliance Measurement: The infosec team will use a variety of techniques, including but not limited to routine walkthroughs, video monitoring, business tool reports, internal and external audits, and reporting to the policy owner, to ensure that this policy is being followed.

5.2 Exceptions: The Infosec team must beforehand approve any exception to the policy.

5.3 Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

- Password Construction Guidelines

7. Revision History

Version	Date	Description
1.0	01-02-2023	Initial Policy