|  |  |
| --- | --- |
| Password Protection Policy | Icon  Description automatically generated |

**Last Update**: *September 2020*

# Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to <Company Name> systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

# Purpose

The purpose of this policy is to establish a standard for strong password creation and protection.

# Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

# Policy

## Password Creation

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

### 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.

### 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 multifactor authentication be used for any privileged accounts.

## Password Change

### Passwords should be changed only when there is reason to believe a password has been compromised.

### Password cracking or guessing may be performed on a periodic or random basis by the <Company Name> or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

## Password Protection

### 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.

### Passwords must not be inserted into email messages, alliance cases or other forms of electronic communication, or revealed over the phone to anyone.

### Passwords may be stored only in “password managers” authorized by the organization.

### Do not use the “Remember Password” feature of applications (for example, web browsers).

### Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

## Application Development

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

### Applications must support authentication of individual users, not groups.

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

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

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

## Multifactor Authentication

### Multifactor authentication is highly encouraged and should be used whenever possible, not only for work-related accounts but also for personal accounts.

# Policy Compliance

## Compliance Measurement

<Company Name> will verify compliance to this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by <Company Name> in advance.

## Non-Compliance

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

# Related Standards, Policies and Processes

Password Construction Guidelines

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
|  |  |  |