|  |  |
| --- | --- |
| Password Construction Guidelines | Icon  Description automatically generated |

**Last Update**: *September 2020*

# Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data or network. This guideline provides best practices for creating secure passwords.

# Purpose

The purpose of these guidelines is to provide best practices for the creation of strong passwords.

# Scope

These guidelines apply to employees, contractors, consultants, and other temporary workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail and local router logins.

# Statement of Guidelines

Strong passwords are long; the more characters you have, the stronger the password. <Company Name> recommends a minimum of 14 characters in your password. In addition, the use of passphrases (passwords made up of multiple words) is strongly encouraged. Examples include “*It’s time for vacation*” or “*block-curious-sunny-leaves.*” Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

* Contain eight characters or less
* Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
* Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321
* Are some version of “Welcome123” “Password123” “Changeme123”

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, <Company Name> highly encourages the use of “password manager” software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

# Policy Compliance

## Compliance Measurement

The <Company Name> security team 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

Any 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

None.

# Definitions and Terms

None.

# Revision History

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