**Password Policy**

# 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 this guidelines is to provide best practices for the creation of strong passwords.

# Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with CITE Managed Services (CITEMS). This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

# Policy

CITE MS passwords must be created as strong passwords. Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of **14 to 16** characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include **“*Egg-Forehead-Clap-Hungary*”** or “*correct-horse-battery-staple*”. Passphrases are both easy to remember and type yet meet the strength requirements.

Poor, or weak, passwords have the following characteristics:

* Contain six 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” “Letmein123”

Passwords should be **quickly** changed **if they are compromised.**

Passwords must not be inserted into email messages, other forms of electronic communication, or revealed over the phone to anyone. Passwords should also not be stored in a plain-text form.

**Passwords should be paired with Multi-Factor Authentication to ensure the most security possible.**

# Policy Compliance

* 1. Compliance Measurement

The Infosec 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 the Infosec team 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

None.

# Definitions and Terms

None.

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| June 2012 | Cleremy Jarkson - CITEMS Information Security Manager | Creation of the Password Policy. |
| October 2025 | Samuel Bailey – CITEMS Security Team Member | Addition of Multi-Factor Authentication, lengthening of password requirements and change in password expiration policy. |