**Password Guideline**

**Last Update Status:** *Updated September 2022*

# 1.0 Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts and company resources. However, a poorly constructed password may result in the compromise of individual/company systems, data, or network.

# 2.0 Purpose

The purpose of this policy is to provide best practices for the creation of strong passwords, the protection of those passwords, and the frequency of change.

# 3.0 Scope

The scope of this policy applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This policy 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.

# 4.0 Policy

# 4.1 General

* All system level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
* All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
* All user-level and system-level passwords must conform to the guidelines described below.

# 4.2 Guidelines

**A. General Password Construction Guidelines**

All users at CIBR Ready should be aware of how to select strong passwords.

Strong passwords are long. The more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases and passwords made up of multiple words. Examples include but are not limited to “*It’s time for a much-needed vacation*” and the password could be “It4@MnVa” or “!T4aMnV@” or some other variation. This password does not meet the minimum characters and is only used as an example. Passphrases are both easy to remember and type. They will also meet the strength requirements. Strong passwords have the following characteristics:

* Contain fourteen characters or more.
* Contain at least three of the five following character classes:
* Lower case characters
* Upper case characters
* Numbers
* Punctuation
* Special Characters (e.g., @#$%^&\*()\_+ etc)

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 and letter patterns such as aaabbb, qwerty, zyxwvuts, or 123321, etc.
* Any of the above spelled backwards.
* Are some versions of “Welcome123” “Password123” “Changeme123”

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

**B. Password Protection Standards**

* Always use different passwords for CIBR Ready accounts from other non CIBR Ready access (e.g., personal ISP account, option trading, benefits, etc.).
* Always use different passwords for various CIBR Ready access needs whenever possible.
* Do not share CIBR Ready passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive, confidential CIBR Ready information.
* Do not reveal passwords in email, chat, or other electronic communication.
* Do not speak about a password in front of others.
* Do not hint at the format of a password (e.g., “my military affiliation”)
* Do not reveal a password on questionnaires or security forms
* Always decline the use of the “Remember Password” features of applications (e.g., Outlook, Google, Messenger).

If an account or password compromise is suspected, report the incident to the Information Security team.

# 5.0 Compliance

**5.1** **Compliance Measurement**

The Information 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.

# 5.2 Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

# 5.3 Non-Compliance

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

# 6.0 Related Standards, Policies and Processes

None.

# 7.0 Definitions and Terms

None.

# 8.0 Revision History

| **Date of Change** | **Responsible** | **Summary of Change** |
| --- | --- | --- |
| December 2020 | D. Cox | 1st Draft |
| March 2021 | P. Clark | 2nd Draft |
| September 2022 | S. Galati | 3rd Draft |