Password Policy

Created by Derell Facey and based on NIST SP 800-63B. Use of this policy or a modified version is allowed. Valid until X/XX/20XX

1.0 Overview

Passwords are used to access accounts and the resources associated with those accounts. Thus, a strong password is important to the security of <*Insert Company Name*> assets and systems, and must be protected. All users (including employees, contractors, and vendors) with access to <*Insert Company Name*> assets and systems are responsible for following the requirements outlined below, when selecting a password.

2.0 Purpose

The purpose of this policy is to define a standard for creating strong passwords and ensuring those passwords remain secure.

3.0 Scope

All individuals who are associated with an account, or credentials for accessing, ant systems within <*Insert Company Name*> facilities, networks, or systems.

4.0 Policy

4.1 General

- Passwords must not contain any strings, greater than 4 characters, that match a string of characters in account email or username.
- Must not match any of the previous 3 passwords.
- All user accounts associated with the network must implement a form of multi-factor authentication (MFA or 2FA).
- Avoid easily guessable/searchable information (e.g., First name, DOB, pet names, street address, etc.)
- Must contain a diverse set of characters (as specified in the guidelines below).

4.2 Guidelines

All employees of <*Insert Company Name*> are required to have strong passwords for all work-related accounts.

Strong passwords adhere to the following requirements:

- Must have at least 8 characters.
- Must have at least 1 upper case letter.
- Must have at least 1 lower case letter.
- Must have at least one digit.
- Must have at least 1 special character (‘#’, ‘.’, ‘?’, ‘*’, ‘/’, etc.).