# IT Password Policy



image

This policy is informed by [NIST Special Publication 800-63B](https://pages.nist.gov/800-63-3/sp800-63b.html)

Version: 1.0

Updated: 10 September 2023

Written by Wyatt Johnson

# Business Level Information

Consider these suggestions for helping to improve your businesses password security:

* Whenever possible, use a password manager. (Keypass and Bitwarden are two examples.) This allows you to easily keep a different password for every website and system, without having to try and remember them all.
* Block or educate employees to not use passwords contained in password dictionaries.
* Lock accounts after multiple invalid login attempts.
* Disallow context-specific words as passwords, such as the company’s name.
* Regularly check employee passwords against breached password lists.
* Reauthenticate user when there is any period of inactivity of 15 minutes or longer.
* Disable the employee’s account immediately upon employment termination.
* Disable accounts when employee is on leave and only enable when employee can authenticate proper dates of return.
* Restrict configuration by implementing least privilege. This means employees will only have access to what they need to complete their responsibility.
* Conducting least privilege audits regularly, making sure that each account does not have more privilege than needed.
* Implement your preferred form of two factor authentication and enforce users to comply to help secure company assets.

# IT Password Policy

## Background

Passwords are the common, basic layer of security when working with computer equipment. This is often how you “prove” to a computer that you are the actual person that is associated with a username. The cybersecurity industry has updated its understanding of what makes a “good password” in recent years to better accommodate how people think and current cybersecurity threats.

## Objective

The goal of this policy is to clearly define the rules that this company has regarding passwords.

## Scope

This policy applies to all employees of this company and has guidelines for both the business and individual employees.

## Policy

* Passwords should be no shorter than 12 characters long. These longer passwords are much harder for computers to “guess”.
* Passwords should be as random as possible. We want passwords that have a high level of entropy, as these are also harder for computers to “guess”.
* Whenever possible, use a password manager. (Keypass and Bitwarden are two examples.) This allows you to easily keep a different password for every website and system, without having to try and remember them all.
* Two factor authentication should be used whenever possible. This is a bit more work when logging in, but makes it much harder for other people to pretend to be you.
* Avoid using repetitive or incremental passwords. The more random a password is, the more secure it becomes.
* Do not use password hints when given the option. This can just end up creating a “back door” for hackers to use.
* Only change your password when necessary. It is better to pick a really good password and stick with it than pick a simpler one and change it frequently.

Employee Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Trainer/Manager Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_