

Password Policy

Overview

Passwords are a key part of our cyber security strategy. The purpose of this policy is to make sure all resources and data receive adequate password protection. We cannot overstate the importance of following a secure password policy and therefore have provided this document for your guidance. The policy covers all users who are responsible for one or more account or have access to any resource that requires a password.

Password Creation:

- All passwords should be sufficiently complex and therefore difficult for anyone to guess.
- In addition, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa\$\$w0rd” are equally bad from a security perspective.
- A password should be unique, with meaning only to the user who chooses it.
- In some cases, it will be necessary to change passwords at certain frequencies.
- Default passwords — such as those created for new users — must be changed as quickly as possible. For example the default password of “funnel123#!#” must be changed **immediately**.