Password Policy Template

Overview

Employees at "CARA Technology" are given access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts in the course of carrying out their duties.

Passwords are a key part of our cyber security strategy and are fundamental to protecting the business and therefore the livelihood of our employees.

All employees who have access to any of those resources are responsible for choosing strong passwords and protecting their own login credentials.

The purpose of this policy is to make sure all "CARA Technology" 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 employees 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. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software controls where possible.
- In addition to meeting those requirements, 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 employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".
- Employees must choose **unique** passwords for all their company accounts and may not use a password that they are already using for a personal account.
- In some cases, it will be necessary to change passwords at certain frequencies. This requirement will be enforced using software when possible.
- If the security of a password is in doubt– for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Protecting Passwords

- Passwords must be **secret**, employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.
- Employees may never share their passwords with anyone internal or external to the business, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognise these attacks.

Storing Passwords

- Employees must refrain from writing passwords down and keeping them at their workstations.
- Employees are encouraged to use password managers but should discuss with the SLT or IT support to agree suitability of chosen application and best use practices.