Password Policy

Company Name

Date

Contents

1 Overview

Passwords are an integral aspect of our computer security program. Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of critical (organisation) resources. As such, all (organisation) staff and outside contractors and vendors with access to our systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3 Scope

The scope of this policy includes all personnel who have or are responsible for an account or any form of access that supports or requires a password on any (organisation) system.

4 Password Policy

4.1 Password Renewal Requirements

- All system level passwords. (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least **every 90 days**.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least **every 90 days.**

4.2 Password Creation Guidelines

- Desktop and mobile devices require a **6 digit** (minimum pin to access them.)
- All other passwords must be a minimum length of **eight (8) characters** on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the User ID.
- Contain both upper and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=`{}[]:”;’?,./)
- It is required that all **administrator accounts** on cloud service must apply multi-factor authentication in conjunction with a password of at least 8 characters.
- Try to create passwords that can be easily remembered. One way to do this is create a password base on a song title, tv show or another phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.
    - NOTE: Do not use either of these examples as passwords!

4.3 MFA

Where MFA (multi factor authentication) is available it must be enabled. MFA can take the form of a text message, a one time access code, notification from an authentication app. For more information see the NCSC’s guidance on MFA.

Where a cloud service does not have its own MFA solution but can be configured to link to another cloud service to provide MFA, the link will need to be configured. A lot of cloud services use another cloud service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace.

4.4 Password Manager

We recommend the use of a password manager for each user.

5 Encouraging Compliance

We have a workflow process which each user goes through to acknowledge they have read and understand and acted based on the policy.

6 Password Compromised

If your password has been compromised, a user must;

- Notify the admin of the organisation.
- Change their password as soon as possible.

6.1 When have passwords been compromised?

Passwords may be compromised if;

- there has been a virus on your system or
- if the manufacturer notifies you of a security weakness in their product. These days, we witness massive credential spills on a day-to-day basis. Whenever such an incident is reported, if you have ever dealt with the victim organization, immediately change the password used.

Passwords exposed in various data breaches worldwide are publicly available as a data dump. Many times, users are not aware when their passwords are exposed in credential spilling attacks. You can use tools such as https://haveibeenpwned.com/Passwords to search if a breached password is being used.

7 Revision History

Version	Revision Date	Summary of Changes
1.0		

8 Document Control

Policy Name	Password Policy
Policy Owner	
Reviewed By	
Review Date	
Review Frequency	