Password and Two Factor Authentication policy

1.0 Overview

This document outlines the password policy for **Conduit Business Solutions Limited**.The policy covers where team members are required to have strong passwords and how to create, store and, as needed, change those passwords. Team members are required to follow this policy to access work networks, accounts and programs.

2.0 Scope

The scope of this policy applies to all team members (**employees and/or contractors)** who have access to or are responsible for an account on any of of Conduit Business Solutions' systems. This includes, but is not limited to: Bit Warden, Microsoft, Xero, Inland Revenue, on-line banking platforms and/or any other client specific applications or software.

3.0 Password length and complexity

Your password needs to be a minimum of **16** characters long and must include:

a) capital letters;
b) lowercase letters;
c) numbers; and
d) symbols.

To create a long but memorable password, combine four or more random words. For example: *dietarygiraffetriangleracetrack*. You can then add numbers, symbols and capital letters at random to increase the complexity or if the application requires it. For example: *dietarygiraFFetriang!erace&track*.

4.0 Creating hard-to-guess passwords

Passwords must not be based on personal information, which could be guessed, such as birthdays, addresses, family or pet names.

Personal information is easy to find online and using it for your password makes it less secure.

Team members should also avoid common passwords (such as such as: "password", "1234567", or "admin") and patterns (such as replacing 'i' with '1' or 's' with '5').

5.0 Unique passwords

Passwords must be unique, both from passwords previously used for that account and passwords used on other accounts. This includes personal accounts. Reusing the same password increases the risk of the account being compromised and can allow attackers to access other systems.

6.0 Multi-factor authentication and verification:

All team members must enable Two-Factor Authentication (2FA) for all company-related systems and accounts where 2FA is available. Preferred methods include authenticator apps (such as Google Authenticator or Microsoft Authenticator) and hardware security tokens, as these provide the strongest level of security. Although SMS-based authentication is permitted when no other method is available, it is acknowledged as less secure and more susceptible to interception. Therefore, SMS-based methods should only be used when no other more secure options are available.

7.0 Frequency of change for passwords

Team members will be required to change their password if it is suspected that their account, or the business network, might be compromised in some way.

8.0 Password protection

Default passwords on equipment (such as WiFi routers) and software should be changed as part of the installation process.

Passwords to individual accounts must not be shared with anyone, including other team members.

Team members must not store passwords in written in a notebook, internet browsers or "remember password" features of applications.

If a team member leaves, any administrator passwords they used or had access to, will be changed.

9.0 Password managers

Team members must use a password manager app to store and create passwords.

Conduit Business Solutions will provide you with an account for **Bit Warden - https://bitwarden.com.**

Team members can use the built-in password manager on their phones only if the phone can only be opened using a password, face ID or fingerprint. For example, keychain on Apple devices. Use a strong password, or passphrase to access it.

10.0 Personal accounts

If a personal account is required to access a work account (for example, to be an admin on a social media platform), the personal account must be secured with the same password requirements as above.

11.0 Handling Compromised Passwords or Two-Factor Authentication (2FA):

If a team member suspects that their password or 2FA has been compromised, they must immediately reset their password, enable new 2FA credentials and ensure the compromised credentials are disabled or revoked.

Team members must also promptly report any issues or suspected compromises with their 2FA setup to rachel@conduit.nz to initiate an investigation to determine the cause and extent of the compromise, assess the risk of data breaches and implement additional necessary security measures.

Affected individuals may receive further instructions to secure their accounts, such as enabling additional verification methods or monitoring for unusual activity. Prompt reporting and swift action are crucial to minimizing potential damage or unauthorized access.