Creating a secure password

1. Introduction

A secure password is your first line of defence against unauthorised access to your personal or professional information. Follow this guide to create secure, memorable, and hard-to-crack passwords.

What Makes a Strong Password?

A secure password should:

- Be at least 8 characters long.
- Include a mix of:
  - **Uppercase letters** (A–Z)
  - **Lowercase letters** (a–z)
  - **Numbers** (0–9)
  - **Special characters** (- @ # $ % ^ & * - ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < >).
- Avoid personal information like your name, birthdate, or common words.
- Be unique — never reuse passwords across multiple account.

Passwords require three out of four of the following categories:

- Uppercase characters
- Lowercase characters
- Numbers
- Symbols.

Passwords not recently used

When a user changes their password, the new password shouldn't be the same as the current password.

Tips for making a strong password

1. **Use a passphrase**

   Instead of a single word, try combining unrelated words into a phrase. Example:

   - BlueMonkey!Drinks7TeaCups

   Passphrases are easier to remember but hard for attackers to guess.

2. **Add complexity**

   Mix up your capitalization, insert symbols, and use intentional misspellings:

   - MyD0gR@n$Fast!

3. **Avoid common pitfalls**

   Do **NOT** use:

   - Simple sequences (123456, abcdef)
   - Keyboard patterns (qwerty, asdfgh)
   - Repeated characters (aaaaaa, 111111)
   - Default or frequently used passwords (password, admin).

Change and manage passwords safely

- **Update passwords regularly,** especially if you suspect a breach.
- Use **different passwords** for different accounts.

Examples of weak passwords

Avoid passwords like:

- password123
- te123456
- welcome1
- kohanga2023
- whanau

DO	DON'T
Use long, complex pass phrases	Using personal info
Mix letters, numbers and symbols	Reusing old passwords