Guide to this document

own your online

This document is a basic template for creating a password policy for your organisation.

How to use it

Any section in square brackets **[like this]** is for you to fill in.

All the policies listed in the document are best practice and recommended by the National Cyber Security Centre (NCSC). You can delete any you feel are not applicable to your organisation.

Note on changing passwords

The NCSC does not recommend changing a strong password unless it has been compromised. Asking staff to regularly change passwords leads to insecure practices, especially repeating patterns or writing down passwords next to the device.

If you are a higher-level user or system administrator, consider reviewing your passwords annually.

Enforcement

Enforcing a password policy is difficult, as you cannot ask to see people's passwords.

The NCSC recommends using positive reinforcement and helping staff understand that a good password is a large part of the battle to keep yourself and the organisation secure.

For more information of building security awareness see CERT NZ's Critical Control on this topic.

Security awareness building | CERT NZ

Basic password requirements

Passwords must be:

- A minimum of 16 characters.
- Not based on personal or guessable information.
- Different to any previously used passwords.
- Different to all other passwords.
- Kept confidential to the user.
- Use a password manager to generate and keep track of passwords.

You can create a passphrase to make this easier – join four or more random words together and add numbers and symbols throughout.

Password policy template

own your online

Overview

This document outlines the password policy for **[Organisation]** .

The policy covers where staff are required to have strong passwords and how to create, store and, as needed, change those passwords.

Staff are required to follow this policy to access work networks, accounts and programs.

Scope

The scope of this policy applies to all staff who have access to or are responsible for an account on any of **[Organisation]** 's systems. This includes, but is not limited to,

[add in core systems - for example: work email, social media accounts, financial systems, customer databases].

Policy

Password length and complexity

Your password needs to be a minimum of **[16]** characters long and must include: capital and lowercase letters, numbers and 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.

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.

Staff 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').

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.

Frequency of change for passwords

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

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 managers or administration staff.

Staff must not store passwords in internet browsers or "remember password" features of applications.

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

Password managers

Staff can use a password manager app to store and create passwords.

[Organisation] will provide you with an account for **[name of password manager].**

Staff 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.

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.