ICT Password Construction Guidelines

Guideline number	4.9	Version	1
Created by	HR & Operations Manager	Created on	9 September 2024
Responsible person	HR & Operations Manager	Scheduled review date	8 September 2025

1. Overview

Secure passwords are critical to the continued security of business operations at NECOM (the Company). Passwords are used in many different parts of the business, for protecting systems, data and devices, and it is essential that passwords are constructed appropriately to ensure that business operations are not compromised to unauthorised parties.

2. Purpose

The purpose of these guidelines is to provide end users with best practice for the creation of strong passwords.

3. Scope

These guidelines apply to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties, who may use passwords to protect data, systems or devices owned by NECOM or with access to data owned by NECOM.

4. Statement of Guidelines

Strong passwords are long. The more characters there are, the stronger the password. As a minimum there should be 14 characters in the password. In addition, we highly encourage the use of passphrases, which are passwords made up of multiple words. Examples include “I can't Believe I have 2 have such a complex password!” or “Square-Hilarious-Cloudy-Squirrels1”. Passphrases are both easy to remember and type, yet meet the strength requirements.

Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less
- Contain personal information such as birthdates, addresses, phone numbers, or names of pets, family members, friends or fantasy characters
- Contain work-related information such as the Company name
- Contain common patterns such as 123, qwerty, zxcv or 999.
- Contain common words or phrases such as ‘welcome’ or ‘password’, including variations such as ‘p@zzW0rd456’.

In addition, every work account should have a different, unique password. To enable users to

maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorised and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

Staff can use their BitWarden password manager to create both random number letter and symbol passwords, and pass phrases. Staff should use the most complex possible password for services they can always use BitWarden to auto fill the password, and should use pass phrases for any passwords that have to be manually entered.

5. Compliance

5.1. Compliance Measurement

The HR & Operations Manager will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. Exceptions

Any exceptions to this policy must be approved by the HR & Operations Manager in advance and have a written record.

5.3. Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Guideline version and revision information

Guideline Authorised by: JLaughton

Title: HR & Operations Manager