ICT Password Policy

Policy number	4.8	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

Passwords are used to protect systems, data and devices across the business. Appropriate and secure use of passwords is essential for business security. Strong passwords significantly reduce the opportunity for unauthorised access to business information resources, whereas weak passwords heighten risks greatly.

2. Purpose

The purpose of this policy is to protect NECOM (the Company) from the threats stemming from weak passwords and inappropriate use and sharing of passwords. These threats include loss of NECOM data, tampering of NECOM devices and systems, cost of recovering data, as well as the potential of regulatory fines.

3. Scope

The scope of this policy includes all employees, temporary workers, contractors and other personnel who use NECOM systems or devices or access NECOM's data or network.

4. Policy

4.1. Password Creation

4.1.1. All passwords must conform to the Password Construction Guidelines.

4.1.2. A separate, unique password must be used for each separate account on the Company's devices, network or systems.

4.1.3. Passwords may not be reused for other applications within the Company or in personal use.

4.1.4. User accounts that have system-level privileges granted through group memberships or programs such as sudo (Admin rights) must have a unique password from all other accounts held by that user to access system-level privileges. In addition, users should always use multi-factor authentication for accounts with system-level privileges when it is available.

4.2. Password Change

4.2.1. Passwords should be changed only when there is reason to believe that the password has been compromised.

4.2.2. Password cracking or guessing may be performed on a periodic or random basis by the IT team or approved delegates. If a password is guessed or cracked during one of these tests, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3. Password Protection

4.3.1. Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential information.

4.3.2. Passwords must not be inserted into email messages, texts or any other form of electronic or non-electronic communication, including over the phone.

4.3.3. Passwords may be stored only in BitWarden only.

4.3.4. Any user suspecting that their password may have been compromised must report the incident and change the password as soon as reasonably feasible.

4.3.5. Passwords must never be stored in the web browsers save password feature.

4.3.6. Passwords must never be written down or otherwise printed on a physical medium.

4.4. Multi-Factor Authentication

Multi-factor authentication must be used whenever possible, especially for systems that have access to sensitive data.

4.5. Password Manager

4.5.1. Staff must use the approved password manager BitWarden to securely store their passwords for accessing the Company's devices, network or systems.

4.5.2. Staff are required to use a password that conforms to the Password Construction Guidelines as their master password.

4.5.3. Staff are required to use Multi-Factor Authentication for their BitWarden account.

4.5.4. Staff can use the password generation feature in BitWarden to create unique passwords for their other accounts.

4.5.5. You must not store your master password within BitWarden.

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.

Policy version and revision information

Policy Authorised by: GMoin

Title: Chairman of the Board