Security Awareness Training Policy

Policy number	4.10	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

Exposure of sensitive business information or personal customer details can be highly damaging to NECOM (the Company). NECOM devices and the NECOM network are also at risk from ransomware and malware attacks, which can prove highly costly to deal with. To prevent breaches of data, infection of NECOM devices or intrusion of the NECOM network, it is essential that all employees, contractors and other users of the NECOM network and devices are trained in the necessary measures to keep up security.

2. Purpose

The purpose of this policy is to set out why it is important for all network and device end users within NECOM to take up security awareness training, and to clearly outline the expectations of employees to engage in their training. This policy will both ensure that employees know what is expected of them, and that NECOM can take necessary measures to uphold compliance with its data protection regulatory requirements.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties, who have access to NECOM's private or personal data, NECOM's network, or devices owned or controlled by NECOM.

4. Policy

All employees of the company must be aware of their responsibilities in protecting the data, devices and network of the company.

The company will provide training to all employees before, and during their use of, the company network and company devices. All new employees will receive a gap analysis questionnaire that will gauge their current knowledge on security areas. Employees will then be trained by individualised programmes that will address their weakest areas first.

Training will be sent out regularly, in the form of online training courses. These courses will be sent out by email and accessed from the company email inbox.

Employees are expected to complete all training courses received by them within no more than 20 working days.

The training will educate employees on the risks of, or best practices regarding the use of, the following core information security areas:

- Email and internet use
- Phishing
- Social engineering

- Malware
- Adware and spyware
- Ransomware
- Working remotely
- Physical security
- Cloud security
- Passwords and authentication
- Social media use
- Voice- and text-based phishing

If an employee has not received training in their email inbox, or they have trouble accessing or completing their training, they must contact their IT support team with no undue delay.

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