Acceptable Use Policy – NECOM devices

Policy number	4.5	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

Most businesses now depend on computers and mobile devices as part of their daily business operations. It is essential, however, to ensure that computers and devices owned or controlled by the business are used in an appropriate, safe and secure manner.

Inappropriate or insecure use of NECOM (the Company) computers and devices could lead to a malware infection, a breach of data, or damage to NECOM's reputation. This is why an Acceptable Use Policy is essential, as it sets out clear rules on the acceptable use of NECOM computers and devices.

2. Purpose

The purpose of this policy is to set out rules on the acceptable and secure use of computers and mobile devices owned, leased, or otherwise controlled by NECOM.

3. Scope

This policy applies to all employees, contractors, temporary workers and any other personnel that may use computing devices or network resources owned, leased or controlled by NECOM or on behalf of NECOM.

4. Policy

4.1. General Use

4.1.1. Company data stored on computing devices owned or controlled by the company remain the sole property of the Company.

4.1.2. The Company's data must be protected in accordance with the Data Protection Standard.

4.1.3. Company data must only be accessed, used or shared only to the extent it is necessary for performing your assigned job duties.

4.1.4. Loss, theft or unauthorised disclosure of Company data must be reported without undue delay to the IT team and line manager.

4.1.5. Personal use of Company computing devices is not entirely prohibited but must be limited to occasional and minimal use that does not interfere with job duties or risk exposure of Company data or systems.

4.1.6. Personal use of Company computing devices is a privilege that can be withdrawn at the discretion of the Company and its IT team at any time.

4.2. Prohibited Use

All illegal, immoral, offensive or intolerant behaviour and content are strictly prohibited on the Company computing devices and network.

The following sections form a non-exhaustive list of prohibited activities and content that are expressly prohibited on the Company network and computing devices.

The following activities are strictly prohibited.

4.2.1. The introduction of malware, viruses, or other malicious programs or applications into Company computing devices or the Company network.

4.2.2. Violation of any copyright, patent, trade secret or other intellectual property.

4.2.3. Using, copying, sharing or accessing copyrighted entertainment, software or other material in an unauthorised manner**.**

4.2.4. Using, creating, transmitting, sharing or accessing material that could be construed to violate sexual harassment or hostile workplace laws, policies or principles.

4.2.5. Posting on any online forum, social media or newsgroup as a representative or associate of the Company without the appropriate permission to do so, or without a disclaimer stating that the opinions expressed are not necessarily held by the Company.

4.2.6. Disclosing any passwords on user or system accounts in the Company's network, devices or systems to any other party.

4.2.7. Allowing your user accounts in the Company's network, devices or systems to be used by others.

4.2.8. Port scanning, security scanning or network monitoring without the express permission of the IT Department.

4.2.9. Circumventing user authentication.

4.2.10. Any form of harassment, abuse, or bullying over email, social networks or in any other form.

4.2.11. Creation or the forwarding of chain letters or multi-level-marketing schemes.

4.2.12. Unauthorised use or forging of email header information.

4.2.13. Unauthorised use of any business email account for purposes not relevant to job duties or for making fraudulent offers or communications.

4.2.14. Engaging in any online activity that may harm or tarnish the image or reputation of the Company, its employees, partners or other associates.

4.2.15. The installation of software not prior approved by the HR & Operations Manager.

4.2.16. Gaining unauthorised access to any other computer or computer network.

4.2.17. Use NECOM devices and or equipment for personal gain, i.e. running a personal business.

4.3. Security

4.3.1. All users on the network must be given minimal access to data and privileges, with only the required access to carry out their role and duties to be given to each user.

4.3.2. All users must set a unique password for their accounts.

4.3.3. All computers must be locked or shut down when they are not in use, even for brief periods.

4.3.4. All computing devices must be set to automatically lock after no more than ten minutes of inactivity.

4.3.5. Users must not save passwords in their browser, only the approved password manager BitWarden may be used.

4.3.6. Where possible all users must use Multi-Factor Authentication on their accounts.

4.3.7. Users in possession of NECOM computing equipment must at all times ensure that it is stored or placed in areas with minimal possibility of theft or damage.

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