Anti-Malware Policy

1. Overview

NIAB is obliged to ensure its computers and network are secure and free from malware. This policy sets out responsibilities for users of NIAB's devices, any device that is used to access company data or conduct company business, or any device used to access the company network.

'Malware' as referred to in this policy includes all types of malicious programs, applications and scripts, including but not limited to viruses, trojans, ransomware, spyware and adware. Malware infections can be costly for the company to deal with, and lead to breach of sensitive data as well as reputational damage to the company. It is essential that all employees take the anti-malware measures set out in this policy seriously, and take all reasonable efforts to protect company devices and the company network.

2. Purpose

The purpose of this policy is to protect company devices and the company network from malware by setting out clear rules, guidelines and responsibilities for all users of company devices and the company network.

3. Scope

The scope of this policy includes all employees, contractors, temporary workers and other personnel who may use company devices or the company network or use any device to access company data or conduct company business.

4. Policy

4.1. All computers that are owned or leased by the company or connect to the company network must run an approved and up-to-date anti-malware program that continually monitors for malicious software.

4.2. As software updates to anti-malware programs are released, they must be downloaded and installed without undue delay.

4.3. Files, attachments and macros attached to emails from unknown, suspicious or untrustworthy sources should never be opened.

4.4. Report any unknown, suspicious or untrustworthy emails and/or attachments you receive to the relevant department or your manager without undue delay.

4.5. Delete all spam, chain, and other junk email without forwarding, in line with the Company's Acceptable Use Policy.

4.6. Never download files from unknown or suspicious sources or websites.

4.7. Never plug in an unknown USB storage device or other removable device to your computer.

4.8. Always report any unaccounted for or unknown removable devices to your manager or the relevant department.

4.9. Only install applications onto your mobile devices from official application stores.

5. Compliance

5.1. Compliance Measurement

The IT team 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 IT team 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.