Virus Protection and Prevention Policy

1.0 Purpose

To establish requirements, which must be met by all personal computers, laptop computers and workstations, connected to Kelvin TOP-SET Ltd networks (either from within the corporate network or remotely), to ensure effective virus detection and prevention.

2.0 Scope

This policy applies to all Kelvin TOP-SET Ltd personal computers, laptops and workstations that belong to or are leased by Kelvin TOP-SET Ltd, or are owned by staff, contractors, casuals, vendors and are connected to the Kelvin TOP-SET Ltd network.

3.0 Policy

3.1 Implementation Policy

1. All Kelvin TOP-SET Ltd computers must have Kelvin TOP-SET Ltd.'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up to date. Virus-infected computers must be removed from the network until they are verified as virus-free. Where operational staff encounter difficulties in installing the latest anti-virus software on legacy clients and servers they should contact Kelvin TOP-SET Ltd IT Staff for guidance.

2. Kelvin TOP-SET IT Staff are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

3. Any activities with the intention to create and / or distribute malicious programs into Kelvin TOP-SET Ltd's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

3.2 Policy Recommendations

Recommended processes to prevent virus problems:

1. Always run the corporate standard, supported anti-virus software.

2. NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

3. Delete spam, chain, and other junk email without forwarding, in line with Kelvin TOP-SET Ltd.'s Acceptable Use Policy.

4. Never download files from unknown or suspicious sources.

5. Avoid direct disk sharing with read / write access unless there is absolutely a business requirement to do so.

6. Always scan external storage media device from an unknown source for viruses before using it.

7. Back-up critical data and system configurations on a regular basis and store the data in a safe place.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
A contractor found to have violated this policy would be liable to their contract to provide a service terminated.

5.0 Definitions

Term	**Definition**
Virus	A software program capable of reproducing itself and usually capable of causing harm to files or other programs on the same computer.
Trojan	An apparently useful or innocent program containing additional hidden code which allows the unauthorised collection, exploitation, falsification, or destruction of data.
Spam	To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages in mass quantities.

6.0 Revision History

Who	Date	Revision Type	Revision Number
Scott Bowden	20/10/2021	Initial draft	V0.1
Scott Bowden	14/03/2022	Updated	V0.2
Scott Bowden	30/01/2024	Annual check/update	V0.3