COMPUTER AND INFORMATION SECURITY POLICIES

Kelvin TOP-SET Ltd has issued new computer and information security policies, which affect all users – including employees and contractors that use the company's computer systems. They include details of acceptable use of the internet, email, and instant messaging systems at work and for those who have remote access to the company network.

The policies are designed to protect Kelvin TOP-SET employees, contractors, and the company itself from illegal or damaging actions by individuals, either knowingly or unknowingly. Any employee found to have violated the security policies may be subject to disciplinary action, up to and including termination of employment.

Key points:

Personal use of the Internet, email and instant messaging systems is acceptable provided that such use does not interfere with employees' work. This also includes the use of music streaming services including but not limited to iTunes, Spotify and Amazon Music.

You should not share or otherwise divulge information (including account details, passwords, and data) to any third party or unauthorised member of staff.

You must not load unauthorised software, games, music, videos, or films onto your computer

You must not actively engage in sourcing or transmitting material that is sexually explicit and/or potentially offensive to others (i.e., any obscene, racist, or criminal materials or any materials inconsistent with the company's values and policies).

If you receive an email and / or attachment which you believe to be offensive or illegal or contains images that you believe may be offensive or illegal email webmaster@kelvintopset.com

You must not send unsolicited or "junk" emails or undertake any form of harassment via mail, telephone, or Instant Messaging. You must not create or forward "chain letters", joke emails or images, or emails relating to "pyramid" schemes.

You should always back up regularly, either to a local storage device or your designated network drive by copying documents/files to your desired backup destination. All machines connected to the corporate network are backed up on a daily basis to the on site server.

Do not connect equipment (including but not limited to an iPhone, iPad, PDA, BlackBerry, MP3 player or USB storage device) to your PC unless it has been provided or is approved for that purpose by IT.

If you are victim of a security incident or wish to report a security breach, email webmaster@kelvintopset.com

Associated Policies

01	**Virus Protection and Prevention Policy**
02	**Internet Usage Policy**
03	**Mobile Computing Policy**
04	**Email and Instant Messaging Policy**
05	**Information Protection Policy**
06	**Password Protection Policy**
07	**Perimeter Security Policy**
08	**Remote Access Policy**
09	**Wireless Communications Policy**
10	**Server Security Policy**
11	**Computer and Information Security Policy**
12	**Personal Communications Policy**

Revision History

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