Mobile Computing Policy

1.0 Purpose

The purpose of this policy is to establish an authorised method for controlling mobile computing and storage devices that contain or access information resources at Kelvin TOP-SET Ltd.

2. 0 Background

With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs of Kelvin TOP-SET Ltd. However, these devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at Kelvin TOP-SET Ltd.

3.0 Scope

Kelvin TOP-SET Ltd employees, consultants, vendors, contractors, casuals, and others who use mobile computing and storage devices on the network at Kelvin TOP-SET Ltd.

4.0 Policy

1. It is the policy of Kelvin TOP-SET Ltd that mobile computing and storage devices containing or accessing the information resources at Kelvin TOP-SET Ltd must be approved prior to connecting to the information systems at Kelvin TOP-SET Ltd. This pertains to all devices connecting to the network at Kelvin TOP-SET Ltd, regardless of ownership (i.e., those provided by the company, a third party or belonging to an individual). Any device accessing information from the systems at Kelvin TOP-SET Ltd must have active and up to date anti-virus software running on it.

2. Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, universal serial bus (USB) port devices, compact discs (CDs), digital versatile discs (DVDs), flash drives, modems, handheld wireless devices (including “BlackBerry’s” and mobile telephones), wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or company / third party owned, that may connect to or access the information systems at Kelvin TOP-SET Ltd.

3. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at Kelvin TOP-SET Ltd unless the Kelvin TOP-SET Group IT department has already approved the media type. Kelvin TOP-SET IT Staff will maintain a list of approved mobile computing and storage devices.

4. Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the network at Kelvin TOP-SET Ltd. Accordingly, portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive Kelvin TOP-SET Ltd information must use encryption or equally strong measures to protect the data while it is being stored.

5. Unless written approval has been obtained from Kelvin TOP-SET IT Staff, databases, or portions thereof, which reside on the network at Kelvin TOP-SET Ltd, shall not be downloaded to mobile computing or storage devices, except for the purposes of syncing mail and calendars.

6. IT staff and users, which include employees, consultants, vendors, contractors, temporaries and casuals, shall also have knowledge of, and adhere to, the Remote Access Policy and Wireless Communication Policy.

7. No portable device shall be brought onto company premises unless previously tested for portable appliance electrical requirements and furthermore checked by IT for compliance with data security.

5.0 Security

Loss or theft of a mobile computing and storage device must be reported to the Kelvin TOP-SET IT Staff immediately. Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by the Kelvin TOP-SET Ltd IT Staff.

Before connecting a mobile computing or storage device to the Kelvin TOP-SET Ltd network, users must ensure it is on the list of approved devices issued by Kelvin TOP-SET IT Staff.

6.0 Enforcement

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

Commented [JG1]: Again, there should be a reference to what may happen if you are not an employee i.e. termination of contract to provide a service

Commented [SB2R1]: Added

7.0 Definitions

Term	**Definition**
Flash Drive	A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. The computer automatically recognizes the removable drive when the device is plugged into its USB port. A flash drive is also known as a USB drive.
PDA	A handheld device ("Personal Data Assistant") that combines computing, telephone / fax, and networking features.
Mobile Devices	Mobile media devices include, but are not limited to PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

7.0 Revision History

Who	**Date**	**Revision Type**	**Revision Number**
Scott Bowden	19/10/2021	Initial draft	V0.1
Scott Bowden	14/03/2022	Updated	V0.2
Scott Bowden	30/01/2024	Annual check	V0.3