Remote Access Policy

1.0 purpose

The purpose of this policy is to protect Kelvin TOP-SET Ltd's electronic information from being inadvertently compromised by authorised personnel using a remote connection. The remote connection may be via the telephone network, Remote Access Virtual Private Network (VPN) connection, using either IPSec or SSL encryption to the Kelvin TOP-SET Ltd corporate network.

2.0 Scope

The scope of this policy is to define appropriate remote access and its use by authorised personnel. This policy applies to all Kelvin TOP-SET Ltd authorised personnel, Kelvin TOP-SET Ltd owned or personally owned laptop computers, personal computers or workstations used to connect to the Kelvin TOP-SET Ltd network. This policy applies to remote access connections used to do work on behalf of Kelvin TOP-SET Ltd, including reading or sending email, accessing network, and / or viewing Intranet / Internet, resources.

3.0 Policy

1. Kelvin TOP-SET Ltd employees and authorised third parties (contractors, vendors, etc.) can use remote connections to gain access to the corporate network. All access is controlled using individual usernames and passwords. No VPN access is given as this is done through a secure shared connection direct to the filestore.

2. Remote Access use is to be controlled using password authentication. The connection is done through a secure cloud connection using Synology services.

3. In the case of access via VPN, the user will either be provided with an account with the Company's preferred Internet Service Provider (ISP) if he / she does not have an existing solution in place or may utilise an existing service provider if already installed and configured. In the event of an existing service provider being used it will remain the users responsibility to pay for and maintain that service.

4. Users of computers that are not Kelvin TOP-SET Ltd owned equipment must have their equipment configured to comply with Kelvin TOP-SET Ltd's policies and at a bare minimum have active and up to date anti-virus software installed and running.

5. It is the responsibility of employees with VPN access privileges to ensure a connection to Kelvin TOP-SET Ltd is not used by non-employees to gain access to Company information system resources. An employee who is granted access privileges must remain constantly aware that VPN connections between their location and Kelvin TOP-SET Ltd are literal extensions of Kelvin TOP-SET Ltd's corporate network, and that they provide a potential path to the Company's most sensitive information. The employee and / or authorised third party individual must take every reasonable measure to protect Kelvin TOP-SET Ltd's assets. This includes not using public/free WiFi such as hotels and to gain a connection, and instead must be paired with their own personal or company mobile phone.

6. General access to the Internet for recreational use by immediate household members through the Kelvin TOP-SET Ltd supplied Internet services on personal computers is permitted. On no account should this access be via a connection into the Kelvin TOP-SET Ltd corporate network. The Kelvin TOP-SET Ltd employee is responsible to ensure the family member does not violate any Kelvin TOP-SET Ltd policies, does not perform illegal activities, and does not use the access for outside business interests. The Kelvin TOP-SET Ltd employee bears responsibility for the consequences if the access is misused. At no

time should any Kelvin TOP-SET Ltd employee provide his or her login or email password to anyone, not even family members.

7. Kelvin TOP-SET Ltd employees and other authorised users with remote access privileges must ensure that their Kelvin TOP-SET Ltd-owned or personal computer or workstation, which is remotely connected to Kelvin TOP-SET Ltd's corporate network, is not connected to any other network at the same time; with the exception of personal networks that are under the complete control of the user to access the Internet in order to establish a VPN connection.

8. Kelvin TOP-SET Ltd employees and contractors with remote access privileges to Kelvin TOP-SET Ltd's corporate network must not use non-Kelvin TOP-SET Ltd email accounts (i.e., Hotmail, Gmail, Yahoo, AOL), or other external resources to conduct Kelvin TOP-SET Ltd business, thereby ensuring that official business is never confused with personal business.

9. Reconfiguration of a home user's equipment (including non-standard hardware configurations) by anyone other than an authorised member of the Kelvin TOP-SET Ltd IT Staff is not permitted at any time.

10. All PCs, laptops and workstations that are connected to the Kelvin TOP-SET Ltd internal networks via remote access technologies must use the most up-to-date anti-virus software; this includes personally owned computers.

11. Personal equipment that is used to connect to Kelvin TOP-SET Ltd's networks must meet the requirements of Kelvin TOP-SET Ltd-owned equipment for remote access.

12. Analogue and non-GSM digital mobile phones cannot be used to connect to Kelvin TOP-SET Ltd's corporate network, as their signals can be readily scanned and / or hijacked by unauthorised individuals. Only GSM standard, 4G and 5G digital mobile phones are considered secure enough for connection to Kelvin TOP-SET Ltd's network. For additional information on wireless access to the Kelvin TOP-SET Ltd network, consult the Wireless Communications Policy.

13. Remote accounts are considered 'as needed' accounts. Account activity is monitored, and if a remote account is not used for a period of six months the account will expire and no longer function. If remote access is subsequently required, the individual must request a new account as described above.

4.0 Foreign Travel

While traveling abroad users must take into account the limitations imposed on the export of encryption technology to certain countries. This means that it is illegal to take Kelvin TOP-SET VPN software into these countries. Users should check with the Kelvin TOP-SET Ltd IT Staff when they are planning to travel abroad taking equipment with remote access capability.

5.0 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.

6.0 Definitions

Term	**Definition**

Remote Access	Any access to Kelvin TOP-SET Ltd's corporate network through a non-Kelvin TOP-SET Ltd controlled network, device, or medium.
Passphrase	Similar to a password but can be made up of any number of characters.
GSM	Global System for Mobile Communications, the most common digital telephony network.
4G	*The fourth generation of broadband cellular network technology.*
5G	*The fifth generation of broadband cellular network technology.*
Remote Access IPSec	Internet Protocol Security, a framework of open standards for ensuring secure private communications over the Internet.
SSL VPN	Secure Socket Layer Virtual Private Network used to provide secure connectivity across the Internet.

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