Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned, leased and / or operated by Kelvin TOP-SET Ltd. Effective implementation of this policy will minimise unauthorised access to Kelvin TOP-SET Ltd proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned, leased and / or operated by Kelvin TOP-SET Ltd, and to servers registered under any Kelvin TOP-SET Ltd owned internal network domain. This policy is specifically for equipment on the internal Kelvin TOP-SET Ltd network.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at Kelvin TOP-SET Ltd must be owned by Kelvin TOP-SET IT Staff that are responsible for system administration. Approved server configuration guides must be established and maintained by Kelvin TOP-SET IT Staff, based on business needs.

Kelvin TOP-SET IT Staff should monitor configuration compliance and implement an exception policy. Kelvin TOP-SET IT must establish a process for changing the configuration guides, which includes review and approval by Kelvin TOP-SET Ltd annually.

Servers must be registered within the asset register. At a minimum, the following information is required to positively identify the point of contact:

1. Server contact(s) and location, and a backup contact

2. Hardware and Operating System / Version

3. Main functions and applications, if applicable

3.2 General Configuration Guidelines

1. Operating System configuration should be in accordance with approved Kelvin TOP-SET Ltd Group IT guidelines.

2. Services and applications that will not be used must be disabled where practical.

3. Access to services should be logged and / or protected through access-control methods such as TCP Wrappers, if possible.

4. The most recent security patches must be installed on the system in accordance with the Kelvin TOP-SET Ltd IT patching policy.

5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

6. Always use standard security principles of least required access to perform a function.

7. Do not use root when a non-privileged account will do.

8. If a methodology for secure channel connection is available (i.e. technically feasible), privileged access must be performed over secure channels, (e.g. encrypted network connections using SSH or IPSec).

9. Servers must be physically located in an access-controlled environment.

10. Servers are specifically prohibited from operating from uncontrolled / unsupervised office or cubicle areas.

3.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

1. All security related logs will be kept online for a minimum of 1 week.

2. Daily incremental digital backups will be retained for at least 1 month.

3. Weekly full digital backups of logs will be retained for at least 1 month.

4. Monthly full backups will be retained for a minimum of 1 year.

Security-related events must be reported to the Kelvin TOP-SET Ltd IT Staff, who will review logs and report incidents to senior management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

1. Port-scan attacks.

2. Evidence of unauthorised access to privileged accounts.

3. Evidence of frequent attempts at password cracking.

4. Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

Authorised persons within Kelvin TOP-SET Ltd will perform audits on a regular basis. The Kelvin TOP-SET Ltd IT Staff or an approved external provider will manage the audits. Kelvin TOP-SET Ltd IT Staff will present the findings to Senior Management and the appropriate support staff for remediation or justification. Every effort will be made to prevent audits from causing operational failures or disruptions.

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
Server	For purposes of this policy, a Server is defined as an internal Kelvin TOP-SET Ltd Server. Desktop machines and test equipment are not relevant to the scope of this policy.
SSH	Developed by SSH Communications Security Ltd., "Secure Shell" is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.
IPSec	IPSec (Internet Protocol Security) is a developing standard for security at the network or packet-processing layer of network communication.
TCP Wrappers	A secure form of the TCP protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over 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