Perimeter Security Policy

1.0 Purpose

The purpose of this policy is to establish a policy for the management and maintenance of perimeter security at Kelvin TOP-SET Ltd.

2. 0 Background

There is a risk that equipment; devices and information held within the Kelvin TOP-SET Ltd corporate network could become compromised due to weaknesses within the inherent design of the security perimeter or through poor management and maintenance of equipment and devices on that perimeter.

3.0 Scope

This policy covers the procedures for requesting a perimeter device configuration change and how the request is approved. Also covered are policies for making such information available and to whom that information can be released.

4.0 Policy

1. It is the policy of Kelvin TOP-SET Ltd that only members of the Kelvin TOP-SET IT Staff responsible for managing and maintaining perimeter security should have day-to-day access to this information. In certain instances this information may be released to internal and external auditors and other authorised persons who may from time to time be involved in the maintenance and configuration of devices such as firewalls.

2. Perimeter device configuration information should never be stored on, or transmitted to, systems of general availability e.g. by email or other unsecured means.

3. All firewall configuration changes will be reviewed by the authorised persons responsible for managing information security within Kelvin TOP-SET Ltd and be subject to change control.

4. Any firewall access has to be requested using the firewall access request form and authorized by a senior partner.

5. Reviews of perimeter security, including external testing (e.g. penetration testing) should be undertaken at least annually.

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
Firewall	A dedicated gateway machine with special security precautions on it typically used to protect a network when it is connected to an outside network, especially the Internet.

Penetration Testing A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker.

7.0 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