LEI SHING HONG LIMITED

NETWORK SECURITY POLICY

Version	Prepared by	Reviewed by	Approved by	Effective Date
1	Corporate MIS	Andrew Won	K.H. Kai	2006-04-10
2	Corporate MIS	Andrew Won	K.H. Kai	2014-03-03
3	Corporate IT	Kevin Yick	Kai-Uwe Seidenfuss	2020-06-22

Objective
The proper operation of the LSH data network (LSH-WAN) is a strategy to achieve success for the LSH group. Because of its strategic importance, the LSH-WAN must be regarded as a critical resource and managed accordingly.

While the Corporate IT function is committed to ensuring its availability, confidentiality, integrity and performance, all LSH entities connected to it must follow and comply with the operational principles and technical standards necessary to achieve these goals.

The purpose of this policy is to define those operational principles and technical standards.

Applicability
This policy applies to all LSH group of companies connected to the LSH-WAN.

Definition and Limits of LSH-WAN
The LSH-WAN includes two parts, the intranet (LSH-WAN-INTRANET) and internet.

The Intranet is aimed at interconnecting all the business entities and organizations belonging to the LSH group. It is made up of an international backbone linking the various countries in which LSH operates. The LSH-WAN-INTRANET encompasses all the telecommunication lines, international nodes and routers. In case lines are not covered by LSH-WAN-INTRANET, organizations and offices may interconnect to form a national/regional network. If the national/regional networks are not in a private environment, the networks are considered as an extranet and are excluded from LSH-WAN-INTRANET.

Firewall must be implemented to protect LSH's network from internet accesses. Firewall must be certified and approved by Corporate IT before it is installed. Internet encompasses lines, nodes and routers up to, and including the LAN port of the corporate routers.

Responsibilities
Both LSH-WAN-INTRANET/ INTERNET are owned by the Corporate IT who is responsible for:

- Defining its architecture, connection topology, addressing scheme, components and equipment.
- Managing, administering and operating it.
- Taking all the measures necessary to keep the connections and prevent from unauthorized access.

Installation and connection of national/regional networks are under the full responsibility of the Business Managing Director and the Operation/Functions Heads who are ultimately responsible for:

- Ensuring the compliance with this policy.
- Taking all the measures necessary to protect the national/regional WAN.
- Preventing any security incident in his/her network from affecting others.

Compliance, Audit and Monitoring
At any time and in order to control the compliance with this policy, the Corporate IT

reserves the right to:

- Audit the connection of a given organization or entity.
- Review the security of that entity.
- Recommend those amendments aimed at improving the security of the connection.
- Monitor the usage of the LSH-WAN.

Noncompliance with this policy will lead to immediate system disconnection and escalation of the issue to the Group Managing Director.

Connecting to and Accessing the LSH-WAN

Only those business entities and organizations controlled by the LSH group are authorized to connect to the LSH-WAN-INTRANET. Others must be connected to internet in order to access LSH's network resources. Connection and use of LSH-WAN requires prior approval from the Corporate IT.

Secure remote access must be strictly controlled and only approved employees and authorized third parties may utilize Virtual Private Network (VPN) to remotely connect to the LSH network to access LSH's network resources:

- VPN gateway is set up and managed by Corporate IT.
- VPN access is controlled by password authentication.
- VPN users will be automatically disconnected from LSH's network after four hours.

Authorized Use, Protocol, Traffic and Services

The LSH-WAN is aimed at supporting the LSH business and it is therefore to be used for business purpose only.

The only transport protocol authorized on the LSH-WAN is the internet protocol (IP). Only TCP services are authorized on the LSH-WAN, i.e. through IP.

These services are managed and made available by the Corporate IT. Access to the network equipment must be authenticated. Only the network administrators in Corporate IT are allowed to access the network equipment. The administrator password of the communication equipment must not be known by anyone other than the staff that manages the equipment.

IP Addressing Schemes

The addressing scheme of the LSH-WAN is defined and managed by the Corporate IT. In order to allow automated procedures, effective technical trouble-shooting as well as security investigations, all other addressing schemes used across the LSH group of companies, especially those of national/regional WAN must be fully compatible with the LSH-WAN. All IP addressing schemes require prior approval from the Corporate IT.

Router Access Lists

Only the static IP addresses approved by Corporate IT will be allowed to access the LSH-WAN routers, i.e. dynamically assigned IP addresses are not allowed to use the LSH-WAN.

All access to the LSH-WAN routers must be explicitly allocated, i.e. default or implicit accesses are strictly forbidden.

Auditable IP Addresses
At all times, Corporate IT and local IT must ensure that IP addresses are linked to an identified workstation, server or a valid equipment.

LSH-WAN Operation
The Corporate IT sub-contracts the operation of the LSH-WAN to an external service provider. All terms and conditions must be described in a contract and a service level agreement (SLA). Both documents follow the ISO standard.

Exceptions to the Policy
All exceptions to this policy must be reviewed and approved by the Head of Corporate IT.

Networking Standards

Corporate Standards	**Remarks**
Network Equipment	
Router	Cisco
Firewall	Juniper / FortiGate – hardware type
	Windows OS built-in – personal firewall
Connection	
Private Network - Intranet	MPLS
Internet / Remote	IPSec/SSL VPN