LEI SHING HONG LIMITED

ANTIVIRUS POLICY

Version	Prepared by	Reviewed by	Approved by	Effective Date
1	Corporate MIS	K.H. Kai	K.S. Gan	2006-04-10
2	Corporate IT	Kevin Yick / Kai-Uwe Seidenfuss	K.S. Gan	2020-06-22

Objective
The LSH group operates hundreds of computers around the world and success of its business depends largely upon the integrity and availability of information stored and processed on these computers. Electronic Viruses represent a threat to this information. Viruses infect computer systems, corrupt data, block network traffic, and break the continuity of business.

The purpose of this policy is to define the measures aimed at preventing the infection and propagation of electronic Viruses, Malware, or malicious code within the group to prevent damage to user applications, data, files, and hardware.

Applicability
This policy applies to all entities, employees and information technology equipment of the LSH group.

Responsibilities
It is the responsibility of everyone who uses LSH's computer network to take reasonable measures to protect the network from Virus infections.

It is the responsibility of the local IT to keep the Virus patterns and signatures updated.

The Business Managing Director and the Operation/Functions Heads are ultimately responsible for ensuring that all the necessary measures are taken to prevent infections by and propagation of electronic Viruses, Malware, or malicious code. In particular, he/she is responsible for informing employees and providing his/her organization with the necessary methods, tools, software updates and procedures.

Definitions

Term	Definition
Computer Devices	They are any type of device connected to a network that could become infected with a computer Virus such as personal computers, servers, laptops, PDAs, etc.
Malware or Malicious Software	It is any program or file that is designed to infiltrate and damage computers without the users' consent. Types of Malware can include computer Viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.
Virus	It is a self-replicating software or script with malicious intent which may cause damage to the operating system of the computer, the storage devices, and any data and/or software stored on it. It is a subset of Malware.

Anti-Virus Software	It is a software that runs on a Computer Device and monitors network connections looking for Malicious Software. Anti-virus Software is generally reactive, meaning a Signature File must be developed for each new Virus discovered and these Virus definition files must be sent to the software in order for the software to find the malicious code.
Virus Definition Files or Signature Files	They are periodic files provided by vendors to update the Anti-virus Software to recognize and deal with newly discovered Malicious Software.

Virus Infection

Viruses can enter LSH's network in a variety of ways:

- **Email**
  By far, most Viruses are sent as email attachments. These attachments could be working documents or spreadsheets, or they could be merely Viruses distinguished as pictures, jokes, etc. These attachments may have been knowingly sent by someone intending to infect LSH's network or by someone who does not know the attachment contains a Virus. However, once some Viruses are opened, they automatically email themselves, and the sender may not know his or her computer is infected.

- **Storage Media**
  Viruses can also spread via various types of storage media. As with email attachments, the Virus could hide within a legitimate document or spreadsheet or simply be distinguished as another type of files.

- **File or Software Download from Internet**
  Downloading file or software via internet can also be a source of infection. As with other types of transmissions, the Virus could hide within a legitimate document, spreadsheet or other type of files.

Prevention and Minimization of Virus Infections

- **Operating System and Platform**
  All computers and servers running the Microsoft Windows products family must be equipped with an Anti-Virus Software which is duly licensed, configured so that the Virus Definition Files are current, routinely and automatically update with the latest viral pattern and signatures, and the Anti-Virus Software must be actively running on these devices.

- **LSH Standard Anti-Virus Software**
  To ensure a consistent and effective prevention, detection, security investigation and installing of curing Viruses across the network, all LSH organizations are required to use one single set of anti-virus products approved by the Corporate IT. Additional security products can be used but should inform Corporate IT.

Anti-Virus Software must only be installed and configured by Corporate/local IT. Users must not delete, disable or interfere with Anti-Virus Software installed on any computer.

Exceptions to this standard must be justified and approved by both local IT manager and the Head of Corporate IT.

- **Functionalities Implementation**
  All scanning functionalities must be resident, i.e. implemented in such a way that any new files are automatically scanned. In parallel, users are allowed to scan files on demand. Regular full scan is scheduled weekly in each LSH's computer and users must wait for the scan to be completed before they start using the computer.

- **Anti-Virus Update**
  The update, if any, should be done automatically every hour to all servers and computers.

Reporting Electronic Viral Infections

Even though all internet traffic is scanned for Viruses and all files on LSH's servers are scanned, the possibility still exists that a new or well-hidden Virus could find its way to a user's computer, and if not properly handled, it may infect LSH's network.

The Corporate/local IT staff will attempt to notify all users under possible Virus threats via email or telephone. Because this notification will automatically go to everyone in the group, employees should not forward Virus warning messages. On occasion, well-intended people will distribute Virus warnings that are actually Virus hoaxes. These warnings are typically harmless. However, forwarding such messages will unnecessarily increase network traffic. All Virus warning messages received from outside (i.e. not from LSH's IT) must be forwarded to Corporate IT for verification. Therefore, users must not distribute these messages to other users by themselves.

As stated, it is the responsibility of all LSH network users to take reasonable steps to prevent Virus outbreaks. They should refer to the following guidelines:

- Do not open unexpected email attachments or links, even from a colleague you know.
- Never open an email attachment from an unknown or suspicious source.
- Never download freeware or shareware from internet without explicit permission of the IT (please see Download Policy for details).
- If a received file contains macros that you are unsure about, disable the macros.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from an unknown or suspicious source.

Infections must be reported to the local IT manager who must in turn take all the measures necessary to:

- Inform all users who are potentially infected.
- Prevent the infection from beginning of propagation within the office or over LSH-WAN.

Notify the IT of Suspicious Files
If you receive a suspicious file or email attachment, do not open it. Inform LSH IT immediately that you have received a suspicious file. The support staff will explain to you how to handle the file.

If the potentially infected file is on a media that you have inserted into your computer, the Anti-Virus Software on your computer may detect a Virus or ask if you wish to scan the media, format the media or eject the media. In this case, eject the media and contact the support staff. They will instruct you on how to handle the media.

After the support staff has neutralized the file, you should send a note to the sender of the file and notify them of the Virus contained in their document.

If the file is an infected spreadsheet, document or presentation that is of critical importance to LSH, the IT will attempt to scan and clean the file if a second copy cannot be obtained from the sender. The IT, however, does not guarantee that an infected file can be totally cleaned and in such case, IT will not allow the infected file to be used on LSH computers.

Exchanging Electronic Data and Mail with Non-LSH Organizations
Special attention must be paid when data and mail are exchanged electronically with non-LSH organizations.

- Scanning must be performed for all incoming electronic data and mails prior to being read or processed on the LSH computers. These measures are particularly indispensable for data and mails downloaded from internet.
- Equivalent scanning process also applies to all outgoing electronic data and mails before they are sent in order to prevent computers of non-LSH organizations from being infected by LSH.