LEI SHING HONG LIMITED

INFORMATION TECHNOLOGY USER 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
To clarify and define the responsibilities of users who are granted access to information technology resources made available by LSH and their obligation to maintain the confidentiality, integrity and availability of these information technology resources.

Information technology resources are used daily to operate the business across the LSH group of companies. It not only represents an investment made by LSH but also is critical to achieving the business objectives of the group in many instances.

The purpose of this policy is to define the basic rules to be applied when accessing and using information technology resources.

Applicability
This policy is applicable to all users of any information technology resources owned, or otherwise operated by/for the LSH group of companies.

Responsibilities
All users are required to comply with the rules stated in this policy.

The Business Managing Directors and the Operation/Function Heads are ultimately responsible for making all users aware of all policies defining their responsibilities in using information technology resources and providing them with the means necessary to comply with those policies.

Definitions

Term	Definition
Information Technology User	Any permanent or temporary staff, contractor, and consultant employed by the LSH group of companies. It also includes employees affiliated with third parties who are authorized to access LSH Information Technology Resources under legitimate or legally valid employment and service contracts.
LSH Information Technology Resources	Any information, data, networks, fixed or portable equipment, computer media, applications, and utilities owned or otherwise operated by/for the LSH group of companies.

Access to and Use of Information Technology Resources
The access to and use of information technology resources is restricted to authorized users.

Such access and use are strictly limited to purposes which are directly and only related to both the business of the LSH group of companies and the user's responsibilities as stated in his/her employment service contract or job description.

Authorized Software
Only licensed software explicitly authorized by Corporate IT and Local Management and purchased by Corporate IT, can be installed or used on LSH computers.

User Identification and Password
Users are responsible for all activities performed using both their personal identifications and passwords. For this reason, users must keep their personal passwords strictly confidential, i.e. they must not share that information with anyone inside or outside the company unless dictated by approved local procedures.

In exceptional circumstance where a personal password must be shared with another party, it must be changed immediately after the need for sharing has expired.

Use of Private Computer, File and Media
Users must not do the followings without prior written consent from their superiors:

- Use their private computers or media for business purposes nor,
- Copy any LSH files or application software to their private computers and media nor,
- Connect any personal network equipment to the LAN or any USB wireless network adaptor to company PC or laptop are strictly prohibited.

Electronic Mail and Ethics
The use of electronic mail either internally or externally is for company business purposes only; personal communications and non-LSH related commercial uses are prohibited. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, MSN Hotmail, etc. to conduct company business or to store or retain company email.

Users should comply with normal standards of professional and personal courtesy and conduct. They should at all times refrain from using the email for lodging personal criticism or complaining the recipient or any third party or of the services/products provided by them. Language, images, or material that can be construed as biased, sexist, racist, harassing, or stressful to employees, clients, and others must be avoided at all times.

Chain Letters
Users must not create or forward any form of chain letters. They must instead retain a copy of such a letter and immediately report to the local IT manager.

Social Media
Blogging and social networking should be done in a professional and responsible manner and ensure that all postings on social media sites adhere to all laws and regulations and at all times follow the LSH policy on social media.

Computer Games
Computer games are prohibited. They must not be accessed online nor introduced or installed on any LSH equipment by any user.

Portable Computers, Accessories and Any Equipment
Users who are provided with the above are required to take all reasonable and available precautions to prevent:

- The computers, accessories and equipment from being stolen or damaged.
- The company information contained therein from being disclosed to

unauthorized persons.

Reporting Misuse and Loss of Information Technology Resources
Users are expected to report immediately to their superiors or to the local IT manager any suspected misuse or loss of information technology resources placed under their responsibility and any suspected compromise of login credentials (such as username, password, etc.), suspected virus or malware infection, or any other suspicious event that may impact the company's information security.

LSH Information Security Measure
Information security measure for LSH computers and communication systems is strictly confidential and must not be disclosed to unauthorized people. When in doubt, the user must seek his immediate superior’s advice.

Clear Screen Policy
In order to reduce the risk of unauthorized access or loss of information, all computing devices must be secured with a password-protected screensaver with the automatic activation feature set to fifteen (15) minutes or less. User must lock the screen or log off when the device is unattended.

Monitoring of Activities
Any user accessing any LSH Information Technology Resource will automatically imply his/her consent to their activities being monitored.

Cybersecurity and Data Protection

The LSH Group has implemented various measures and controls to avoid potential cyber breaches and reduce cyber risks and also taken steps to increase cyber and data protection awareness across the organization.

All companies and Information Technology Users of the LSH Group are to ensure compliance with the respective applicable local and international data privacy laws and regulations (the “Privacy Laws”), and to observe the consequences of breaching the same when transferring data to other companies and/or locations. This not only helps avoid potential lawsuits and regulatory investigations (and possible heavy penalties) involving data security, but also protects the reputation of the LSH Group. These efforts include observing both the relevant Privacy Laws and cyber security laws, and also other local ordinances, acts and regulations (including any amendments or additions thereto) and any new enactments related with to data privacy and protection.

Examples of the aforesaid laws include, but are not limited to, the China Cybersecurity Law, the European General Data Protection Regulation (GDPR), the Australia Privacy Act and its Australian Privacy Principles (APPs), the Hong Kong SAR Personal Data (Privacy) Ordinance, Korea Personal Information Protection Act (PIPA), the Singapore Personal Data Protection Act (PDPA), the Taiwanese Personal Data Protection Act (PDPA), etc.