LEI SHING HONG LIMITED

INFORMATION TECHNOLOGY PERSONNEL 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 misuse, unauthorized disclosure, destruction or alteration, whether intentional or accidental, of information technology systems and resources may cause serious prejudice to LSH business and reputation.

The purpose of this policy is to define the obligations of IT Personnel in safeguarding the security rules and controls during their employment, transfer and departure in protecting the IT assets.

Applicability

This policy is applicable to all Information Technology Personnel employed by the LSH group of companies.

Responsibilities

The Business Managing Directors and the Operation/Function Heads are responsible for ensuring that the procedures followed in their information technology organizations are in compliance with this policy, taking into account any additional or linking local laws and regulations.

Definitions

Term	Definition
Information Technology (IT) Personnel	Any LSH group's permanent, temporary or contract staff employed by the LSH group of companies. The personnel is given specific responsibilities for managing, developing, installing, maintaining and operating LSH information technology facilities, systems, applications and resources.

Information Technology Job Descriptions

All information technology positions are subject to a formal job description. Each job description must clearly specify the position, the tasks and responsibilities of the function as well as the personnel skills and professional qualifications required for performing the function.

The job descriptions must be updated and maintained to reflect organizational changes as required.

Segregation of Duties

Managers responsible for information technology functions must ensure that none of these functions implies contradictory responsibilities that could compromise security or generate conflict of interests (e.g. business responsibilities together with information technology system responsibilities). Exceptions to that rule must be approved by the Head of Corporate IT.

Recruitment of Information Technology Personnel

Managers responsible for the recruitment process of IT Personnel must ensure the maintenance of a clear and up-to-date job description for the job function.

Whenever possible, applications for employment must be screened for satisfactory references and checked for adequate professional qualifications and skills in

accordance with the requirements stated in the job description.

At the conclusion of the recruitment phase, new Information Technology Personnel must be made aware of his/her obligations, responsibilities and the IT policies and rules.

Transfer of Personnel
When Information Technology Personnel are transferred to a new role or function within the group, all their access rights and resources, including equipment, documentation, media, keys and badges must be checked for required continuance.

Former line manager and their superiors must ensure that all those access rights, passwords and resources that were necessary to perform his/her previous duties are immediately revoked, changed or otherwise returned on transfer.

New line manager must ensure that appropriate levels of access rights and resources needed to fulfill his/her new responsibilities are granted.

Departure of Personnel
In order to prevent any potential security exposure, line manager must ensure that all Information Technology Personnel's access rights and passwords are immediately revoked or changed from all relevant systems upon their departure.

All company resources possessed by the departing personnel, including equipment, documentation, media, keys, and badges must be checked and returned before departure.

Confidentiality
Personnel must not disclose to any third party any information gained during the execution of their duties.

Proprietary Information
All data, software and application created by Information Technology Personnel as part of their contractual obligations remain the property of LSH. Consequently, they must not reproduce any of these, totally or partially, for their own or for a third party, without prior consent of their line manager.

Reporting Security Problems and Incidents
Information technology personnel must report immediately to their line manager any security problems, weaknesses, or incidents that they may encounter.

Abuse of Access Rights
By the nature of their activities, Information Technology Personnel have privileged rights to access sensitive, confidential, or personal information. Users' rights are based on the principle of least privilege and strictly limited to the minimum access needed to enable required management and operation of information technology systems.

Any deliberate attempt, whether successful or unsuccessful, to gain access to or manipulate information not intended for them, will be subject to disciplinary action up to and including termination.

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.