LEI SHING HONG LIMITED

ACCESS AND RIGHTS 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

This document contains LSH proprietary information and is supplied for internal use only. It is confidential and shall not be copied or reproduced (other than for internal use), nor disclosed to any other party, without the express permission of LSH.

Objective
Information technology systems and resources are used daily by users to operate the business and achieve the objectives of the group.

To ensure the integrity and availability of those systems and resources, only authorized users are permitted to access and use those systems and resources in strict accordance with their functional responsibilities and tasks. Therefore, procedures must be implemented to manage and control the different stages in the life cycle of users' access rights, from their initial allocation to their final suppression.

Fundamental security principles such as "segregation of duties" and "limited access rights" must be enforced by those procedures to prevent unauthorized access to LSH systems and resources and to reduce risk of negligent or deliberate system misuse.

The purpose of this policy is to establish those requirements necessary to ensure proper control over user access rights.

Applicability
This policy is applicable to all users and information technology personnel employed by the LSH group of companies including those employees affiliated with third parties who are explicitly authorized to access and use any LSH information technology systems and resources.

Responsibilities
The Business Managing Directors and Operation/Function Heads are ultimately responsible for ensuring compliance with this policy.

Allocation of Access Rights
Allocation of access rights applies to new users of any given systems who are assigned an individual user identifier (or account name) and granted the access rights needed to perform the duties.

The allocation of access rights must be supported by a formal request, verified and approved by the user's line manager. The request must provide all necessary information to allow for effective creation of the user identifier and the allocation of the needed access rights (e.g. user's name, function, department, manager's name, requested access rights, etc.)

Line manager must ensure that the required access rights are consistent with the user's functional responsibilities and strictly limited to those resources needed to perform his/her duties. Unless otherwise required and duly approved, access rights resulting in conflicts of interest or plurality of functions must be rejected.

The request must be confirmed by the user to acknowledge receipt of his/her identifier (or account name) and initial password through on-site delivery or by telephone. Requests must be filed and retained for verification and/or other administrative purposes.

Those responsible for creating the user identifications and granting the access rights

must check the request for security clearance. Irregularities or inconsistencies must be reported to the user's line manager for further verification.

Modification of Access Rights
Modification of access rights is required for authorized users whose access rights are modified for organizational or functional reasons.

Modification of access rights must be supported by a formal request which is verified and approved by the user's line manager. The request must provide all necessary information to allow for effective modification of the user's access rights (e.g. user's name, old/new departments or functions, manager's name and functions, access rights change, etc.)

Line manager must ensure on-going consistency between users' access rights and their functional responsibilities in order to align with the principle of segregation of duties and avoid compromising security due to the accumulation of conflicting access rights. Unless otherwise required and duly approved, access rights resulting in conflicts of interest or leading to plurality of functions must be rejected.

The access providers must check the request for security clearance. Irregularities or inconsistencies must be reported to the user's line manager for further verification.

Modification requests must be filed and retained for verification and/or other administrative purposes.

Suspension of Access Rights
Suspension of access rights primarily applies to users temporarily absent for a long period of time (e.g. sick leave, maternity leave, sabbatical leave, short-term assignment, etc.)

To prevent the abusive use of user accounts and associated privileges during the absence of their owners, all accounts remaining inactive for longer than thirty (30) days must be disabled from all relevant systems and re-enabled only on return of their respective owners. The account owner or his/her line manager is responsible for submitting request for the suspension and reactivation of the accounts upon the owner's return.

Suppression of Access Rights
Suppression of access rights applies to those users who change jobs, leave the company or terminate their contracts.

When a user changes job position/function but still remains employed by the LSH group of companies, his/her former manager must ensure that previously granted access rights and associated account(s) are revoked from all relevant systems.

The user's new manager must arrange for a new allocation process as required.

When a user leaves LSH or terminates his/her contract, his/her manager must ensure that all access rights and associated user identification (accounts) are immediately revoked from all relevant systems after the person leaves.

Shared User Identification (Account)
Unless documented and duly approved by local management, shared user identification or account is not permitted.

By approving such a shared access, the line manager takes the full responsibility of monitoring its usage. Where such access is provided, users' consents must be obtained to demonstrate their understanding of the shared responsibility with respect to these identifications or accounts.

Unused User Identification (Account)
All user identifications or accounts not being used must be systematically removed, revoked or otherwise disabled.

Control
For control purposes, information technology personnel in charge of system administration must maintain and be able to produce at any time an exhaustive list of all user identifications or accounts residing on the systems under their responsibility.

User log in/out of LSH's domain network is recorded in LSH's network and the log is reviewed randomly by IT personnel regularly.