LEI SHING HONG LIMITED

PHYSICAL SECURITY AND SAFETY POLICY

Version	Prepared by	Reviewed by	Approved by	Effective Date
1	Corporate MIS	Andrew Won	K.H. Kai	2006-04-10
1.2	Corporate MIS	Andrew Won	K.H. Kai	2017-04-10
2	Corporate IT	Kevin Yick	Kai-Uwe Seidenfuss	2020-06-22

Objective
Information technology facilities and equipment are critical assets of the LSH group of companies. Requirements for security may vary considerably between business locations, depending on the scale and organization of the information technology services provided, as well as the sensitivity or criticalness of the supported business activities.

To preserve LSH investments and prevent business interruption, security measures consistent with the values of services and business activities must be implemented whenever possible to protect information technology facilities and equipment from unauthorized access, damage or loss.

The purpose of this policy is to define the basic security measures aimed at protecting the above assets.

Applicability
This policy applies to all information technology facilities and equipment within the LSH group of companies.

Responsibilities
The Business Managing Director and the Operation/Function Heads are ultimately responsible for ensuring that reasonable precautions are taken to protect their information technology facilities and equipment in compliance with this policy.

Inventory and Accountability of Assets
Information technology organizations in charge of managing assets must establish and maintain an inventory. All information technology assets must be accounted for, i.e. ownership of asset must be identified. When an asset, for example a portable computer, is placed under the responsibility of a user, the relevant information must be filed in the personnel file.

Physical Security

- **Physical Entry Controls**
  Whenever feasible, information technology facilities supporting LSH business activities must be housed in secure areas. To ensure that only authorized personnel are allowed access during and outside normal working hours, information technology facilities must be protected by the following entry controls:
    - Access must be controlled by a control system (e.g. badge card system, key-entry system, etc.)
    - Only persons who need to operate, supervise or provide maintenance to the area and its equipment are allowed to access the server room.
    - Access from outside to the server room must be controlled with proper user identifications (IDs) and passwords which are to be changed regularly. Unused IDs must be deactivated immediately and deleted by specific time of period.
    - Visitors must be supervised by LSH personnel for the time of their visit or intervention.
    - Rights to access must be revoked immediately for staff who leaves

employment or finish the contract.
    - Main entrance to information technology facilities must be locked at all times.

- **Security of Server Room**
  Server room housing critical equipment, such as servers, routers, switches, hubs and firewalls, requires appropriate physical security as follows:
    - Areas must be located away from and not be contiguous to public access areas.
    - Areas must be separated from the other office areas.
    - Areas must not be located close to, nor contain, hazardous and combustible materials.
    - Areas must be free from any water hazards (e.g. flooding, water leakage, etc.)
    - Adequate fire detection and suppression equipment must be installed, taking into account of any applicable local government regulation.
    - Adequate supply of appropriate handheld fire extinguishers must be readily available in all information technology premises to deal with electrical or general fires.
    - Server room supplies, such as stationery and media (e.g. forms, tapes), must not be stored in the server room area.
    - Backup equipment and data backup must be stored securely outside the server room.
    - Doors and windows allowing access to the computer area must be locked when unattended.
    - The server room must be locked at all time.

- **Security of Information Technology Equipment**
  Information technology equipment supporting critical or sensitive business activities must be protected from failure and other environment hazards to prevent business disruption. Adequate protection of the equipment includes the following preventive measures:
    - An uninterruptible power supply (UPS) facility must be installed to support critical processing in the event of fluctuation or failure of the main power supply.
    - The duration of power supplied by the UPS must be sufficient to allow current processing to terminate properly and to action emergency procedures as required.
    - Telecommunication and local network cabling must be installed safely and physically protected against abuse, interception or damage.
    - Information technology and safety equipment must be maintained in accordance with the suppliers' or manufacturers' recommended service interval levels and specifications.
    - Repairs and servicing of equipment must be carried out by authorized maintenance personnel only.
    - Spare parts or maintenance agreements must be arranged to reduce recovery delays of processing services.
    - Damaged devices containing storage media (e.g. hard disks) must be checked prior to disposal or repair to avoid unauthorized used or disclosure of sensitive data or licensed software.

- Smoking, eating, or drinking must be prohibited in areas housing critical information technology equipment.

Server Room Standards and General Operations (Variance in Countries)

- **Server Room Standards**
  - Physical entry control
    - Access to the server room must be controlled by a control system (e.g. badge card system, key-entry system, etc.)
  - Power supply
    - The power supply circuit for the server room equipment must be a unique supply direct from the main distribution panel and must not have other devices attached to it.
    - A backup UPS is required to prevent data loss or equipment damage if the main power fails.
    - Emergency lighting powered with battery charged by AC power supply is required.
  - Air conditioning
    - The server room must have its own air conditioning.
    - The temperature and humidity of the room must be maintained at or below 16°C and 55% RH.
    - The air conditioning system must be operating 24 hours throughout the year.
    - Water leakage must be avoided for ceiling mounted fan coil unit (if used).
    - Fresh air must be introduced in order to create a positive pressure environment to minimize dust penetration from outside.
  - Construction hazards
    - The server room must not be adjacent or close to any natural gas or liquid transporting pipes, water sources, high voltage lines or magnetic radiation sources.
    - A complete airtight enclosure and water flooding prevention are required for the server room.
  - Fire precaution
    - Fire precaution and protection equipment must be installed according to the local regulation. Vendor expertise must be obtained if fire extinguisher is installed in the server room. No liquid form of fire extinguisher should be used in the server room.
    - All materials used in constructing the server room must be fireproof.
  - Smoke detector
    - Smoke detector equipment must be installed in the server room.
  - Data backup
    - Database and file backup will be kept as current as reasonable. Off-site data and software backup will be maintained.
  - Safe location
    - The site of server room must not be located in flood or earthquake area.

- **General Operations**
  - Housekeeping
    - Smoking, eating, or drinking is NOT permitted in the server room.
    - Operations personnel are responsible for maintaining a clean working area.
    - Operators should not attempt to repair any equipment without the specific authorization of the supervisor or maintenance vendor.
    - Operators should not alter programs without specific authorization of the supervisor.
    - The equipment is not used for other-than-assigned operations.
    - Temperature and humidity are to be monitored at all time and kept within the recommended ranges for the equipment.
  - HDs/Tapes handling
    - HDs/tapes must be cleaned in accordance with the manufacturer's recommendation.
    - HDs/tapes are kept in protective containers when not in use.
    - HDs/tapes are stored in a secured off-site location (e.g. safety box of a bank). Only personnel authorized by local IT manager can access the HDs/tapes in the location.
    - Daily backup HDs/tapes are kept as required by local business.
    - The backup HD/tape for each month will be kept as the month-end backup and the HDs/tapes will not be reused.
    - All backup HDs/tapes will be used for maximum 2 years (about 100 times). After 2 years, HDs/tapes will be replaced by new ones and old HDs/tapes will be disposed.
    - All old HDs/tapes will be physically destroyed upon for disposal.
    - All backup HDs/tapes must be labeled appropriately.
  - Daily duties
    - All system messages on the display monitor or in system message log should be checked (see Appendix II for Daily Operations Checklist).
    - The scheduled jobs, if any, should be checked regularly. If there are any incomplete priority jobs, the IT personnel should rearrange the job schedule. If there is a major problem, the IT personnel must report to the superior.
    - Backup tapes for day-end should be checked and reported to the superior should any problem arises.
  - Other responsibilities
    - IT personnel are required to perform system recovery for hardware and/or software failure (see Appendix III for System Failure and Recovery Actions).
    - The systems should be powered up/down. IT personnel may be required to turn the computer systems off/on and perform an IPL (Initial Program Load) procedure.
    - Messages to online users of system downtime should be transmitted.
  - Administrative responsibilities
    - Administration Department should be coordinated to order supply items.
    - Equipment, accessories, suppliers, and manuals should be

maintained.
    - Maintenance, equipment/accessories delivery by vendors should be scheduled.
    - IT related documents such as delivery notes, invoices, etc. should be maintained.

- **Cloud Applications**
    - Cloud applications should be backed up which should be performed by the relevant service provider. These backups are to be defined in the respective service agreements to ensure at least a daily backup is performed.

Appendix I

Backup Procedures

Backup Job 1

Backup Target:
All servers (with exception shown on Backup Job 2)

Backup Schedule:
Monday ~ Sunday (Backup job starts at 6:00 pm)

	MON	TUE	WED	THU	FRI	SAT	SUN
1st Week	☑ Incremental	☑ Incremental	☑ Incremental	☑ Incremental	☑ Incremental	☑ Full	☑ Incremental
2nd Week	☑ Incremental	☑ Incremental	☑ Incremental	☑ Incremental	☑ Incremental	☑ Full	☑ Incremental

Backup Generation:
14 generations / 2 weeks

Remark 1:
The 1st Saturday backup copy for all servers is reserved as Monthly Backup.

Remark 2:
The Monthly Backup will save to a HDD and transfer to HSBC or BOC deposit box for off-site storage.

Backup Job 2

Backup Target:
Whole system backup of servers below:

NC Server(s)

Backup Schedule:
Saturday (Backup job starts on Sunday at 6:00 pm)

	MON	TUE	WED	THU	FRI	SAT	SUN
DB Backup	☑	☑	☑	☑	☑	☑	☑
System Backup							☑

Backup Generation:
Database: 37 generations with off-copies
System: 2 generations / 2 weeks

Remark 1:
The 1st Saturday backup copy for all servers is reserved as Monthly Backup.

Remark 2:
The Monthly Backup will save to a HDD and transfer to HSBC or BOC deposit box for off-site storage.

Appendix II

Daily Operations Checklist

- All event logs for the last 24 hours.
- The real-time performance chart.
- Anti-virus software log.
- The status of disk capacity of all servers.
- Pop-up messages.
- The HD/tape backup logs for last night.

Appendix III

System Failure and Recovery Actions

<table>
<tr><th colspan="2">Actions Taken in Case of System Failure</th></tr>
<tr><td colspan="2">Aim: Clarify whether it is the hardware or software failure.</td></tr>
<tr><td>Hardware problem</td><td>Software problem</td></tr>
<tr><td>1. Inform affected users as soon as possible if daily operations are interrupted.
2. Inform the corresponding hardware support vendor to repair.
3. Start to install/restore the corresponding program/database onto the emergency server.
4. If the original server can be resumed without any data loss, keep it running. All database/program will be uninstalled on the emergency server.
5. If the original server cannot be recovered, the emergency server will serve as temporary production server until the original server is fixed.</td><td rowspan="3">1. Depends on the recommendations from the corresponding software manufacturer, specific methods should be used to recover the back-office software. It may include reinstallation of the programs and restoration of the tape-backup data.</td></tr>
<tr><td>Remarks: After hardware is repaired.</td></tr>
<tr><td>1. Restore everything onto the repaired server.
2. Fall back everything from the emergency server.</td></tr>
</table>

For emergency after office hours, users may contact the local IT for assistance.