LEI SHING HONG LIMITED

MOBILE DEVICE SECURITY POLICY

Version	Prepared by	Reviewed by	Approved by	Effective Date
1	Corporate MIS	K.H. Kai	K.S. Gan	2014-01-07
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.

Background

Adoption of Mobile Devices by business Users has been astonishingly quick. With an increasing number of organizations using mobile technology such as smartphones and other wireless devices, crafting an effective Mobile Device policy is vital. Keeping employees connected at all times requires a policy that ensures not only efficiency and effectiveness, but also data security.

Mobile Devices such as laptops, smartphones and portable storage devices pose a particularly high security risk, primarily because they are vulnerable to theft and loss. Their material value is however of secondary concern when compared to the potential cost of losing or compromising confidential, personal and/or sensitive data.

LSH Mobile Devices are perceived as personal items and are frequently selected, purchased and configured by their end users without consultation with IT support units. While there are numerous technical measures that can be taken to secure data on Mobile Devices, their implementation is not always straightforward and it is recognized that the majority of Users will not establish effective security on their Mobile Device without specialist advice or assistance.

Security controls should be appropriate for the level of information on the device.

Policy Statement

The Corporate IT, seeks to protect LSH Mobile Devices and their data from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

Objective

This document describes the minimum security policy for LSH Mobile Devices. Mobile Devices must be appropriately secured to prevent sensitive or confidential data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the LSH's computing and information infrastructure.

Scope

This security policy applies to the User of any Mobile Device which connects to the LSH managed network / resource.

Definitions

The followings are the terms and definitions for this policy.

Term	**Definition**
Mobile Device(s)	These include, but are not limited to, personal digital assistants (PDAs), notebook computers, tablet PCs, iPhones, iPads, iPods, Palm Pilots, Research in Motion (RIM) Blackberrys, Microsoft Pocket PCs, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs, and other similar devices**.**
User(s)	Anyone with authorized access to the company's business information systems. This includes permanent and temporary employees, third-party personnel such as temporaries, contractors, or consultants, and other parties with valid company access accounts.

Screen Lock	A password-protected mechanism used to hide data on a visual display while the device continues to operate. Screen locks can be activated manually or in response to rules.
Screen Timeout	A mechanism that turns off a device display after the device has not been used for a specified time period.
Personal Information	Information that can be used to identify an individual and/or an individual's financial account(s), credit history, or credit cards, as well as individual medical record and health plan information. This includes an individual's first name (or initial) plus last name along with his/her driver's license number, identification card number, passport number, financial account numbers, and/or credit card numbers.

Enforcement
Noncompliance with this policy and/or its resulting procedures may lead to disciplinary action up to and including discharge, and may involve civil or criminal litigation, restitution, fines, and/or penalties.

Responsibility

- Each User of a LSH Mobile Device is responsible for following this policy and any related policy or procedure promulgated by their Division / Department head.

- Each Division / Department may also establish policies and procedures and assign responsibility to specific personnel to achieve compliance with this policy.

- Anyone observing what appears to be a breach of security, violation of this policy, violation of government regulations, theft, damage, or any action placing LSH resources at risk must report the incident to an appropriate level supervisor, manager, or security officer within their organization. Those reporting alleged incidents will be protected from retaliation by existing whistleblower protection laws.

- Managers and supervisors are responsible for ensuring that Users are aware of and understand this policy and all related procedures.

Policy

- All Mobile Devices must be password protected. Choose and implement a strong password – at least six (6) characters in length.

- The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.

- If a Mobile Device is lost or stolen, promptly report the incident to the proper authorities. Also, be sure to document the serial number of your device now, for reporting purposes, in the event that it is lost or stolen.

- Sensitive or confidential documents, if stored on the device, should be encrypted if possible.

- Mobile Device options and applications that are not in use should be disabled.

- Sensitive and confidential information should be removed from the Mobile Device before it is returned, exchanged or disposed of.

- Whenever possible all Mobile Devices should enable Screen Locking and Screen Timeout functions.

- No Personal Information shall be stored on Mobile Devices unless it is encrypted and permission is granted from the data owner.

- Before a Mobile Device is connected to LSH IT systems, it shall be scanned for viruses (the User risks having files on the device deleted if any viruses are detected). If media Mobile Device is used for transitional storage (for example copying data between systems), the data shall be securely deleted from the Mobile Device immediately upon completion.