LARK TRADING AND FINANCE LIMITED

Information Technology Policy

1. Purpose

In terms of the provisions of Section-B of the Master Direction - Information Technology Framework for the NBFC Sector dated June 8, 2017, ("Master Directions") issued by the Reserve Bank of India (RBI), every Non-Banking Financial Company (NBFC) having asset size less than Rs. 500 crores shall have Board approved Information Technology Policy/Information System Policy. This Information Technology Policy ("**IT Policy**") is a formal document to provide guidance to the management of Lark Trading and Finance Limited ("**LTFL**" / "**Company**") for developing basic IT systems mainly for maintaining the database and follow the basic standards mentioned in the said Directions.

The Master Directions require the NBFCs to formulate and adopt an Information Technology Policy commensurate with the size, scale and nature of the business carried out by NBFC, which will act as a framework for usage of IT resources within the organisation. Accordingly, this IT Policy is adopted by the Board of the Company.

LTFL provides unsecured personal loans digitally and therefore has access to the customer's personal and financial information. To ensure confidentiality, integrity and availability of information, appropriate safeguards need to be in place to protect it from a wide range of threats. It is therefore essential that an appropriate set of controls and procedures are implemented to achieve information security.

2. Reference

In this IT Policy, a reference to the following word(s) shall have following meanings assigned to it:

2.1 Information Technology Resources:
Information Technology Resources for purposes of this IT Policy include, but are not limited to, LTFL owned or those used under licence or contract or those devices not owned by LTFL but intentionally connected to LTFL - owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and internet and intranet access.

2.2 User:
Anyone who has access to Information Technology Resources, including but not limited to, all employees, temporary employees, contractors, vendors and suppliers.

2.3 Password:
A password is a string of characters used for authenticating a user on an Information Technology Resources of LTFL.

3. Policy

The use of LTFL's Information Technology Resources in connection with LTFL's business and limited personal use is a privilege but not a right, extended to various Users. The privilege carries with it the responsibility of using LTFL's Information Technology resources efficiently and responsibly.

By accessing LTFL's Information Technology Resources, the User agrees to comply with this IT Policy. Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject LTFL to any liability. LTFL reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose LTFL to risk of unauthorized access to data, disclosure of information, legal liability, or other potential system failure is prohibited and may result in disciplinary action, including termination of employment and/or criminal prosecution.

4. Scope

This IT Policy applies to everyone who, in India, has access to LTFL's Information Technology Resources and it shall be the responsibility of senior management at the registered office to ensure that this IT Policy is clearly communicated, understood and followed by all Users.

The IT Policy covers the usage of all of the Information Technology Resources and communication resources, whether they are owned or leased by the Company or are under the Company's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which the equipment is connected.
- All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, internet and intranet and other on-line services.
- All software including purchased or licensed business software applications, LTFL-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on LTFL-owned equipment.

This IT Policy also applies to all Users, whether on Company premises or otherwise, connected from remote connections via any networked connection, or using Company's equipment.

5. Access Control

5.1 All Company computers that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.

5.2 All in-bound connections to LTFL computers from external networks must be protected with an approved password or ID access control system. Modems may only be used at LTFL after receiving the written approval of the Head (IT) and must be turned off when not in use.

5.3 All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user.

5.4 Users shall not make copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

5.5 Users are forbidden from circumventing security measures.

5.6 Users are strictly prohibited from establishing dial-up connections, using modems or other such apparatus, from within any LTFL's premises.

5.7 Users who have been given mobile/portable laptop or any other device and duly authorized for such remote access, which connects to LTFL's mail system on a real-time basis, can do so through the Internet.

5.8 Unless the prior approval of the senior management or Head (IT) has been obtained, Users shall not establish internet or other external network connections that could allow non-authorized users to gain access to LTFL systems and information. These connections include the establishment of multi-computer file systems, internet web pages & FTP servers.

5.9 Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the senior management or CIO. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of this IT Policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

6. Passwords

6.1 Individual password security is the responsibility of each user.

6.2 Passwords are an essential component of LTFL's computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.

6.3 To make guessing more difficult, passwords should also be at least eight characters long.

6.4 To ensure that a compromised password is not misused on a long-term basis, Users are encouraged to change passwords every 30 days. Password history would be maintained for previous three passwords. This applies to the Systems Login (windows password) and Cloud Mail passwords.

6.5 Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.

6.6 Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.

6.7 Under no circumstances, Users shall use another User's account or password without proper authorization.

6.8 Under no circumstances, the User must share his/her password(s) with other User(s), unless the said user has obtained from the concerned senior management/Head (IT) the necessary approval in this regard. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.

6.9 In cases where no prior approval had been obtained for sharing of password(s) with other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this IT Policy and LTFL shall initiate appropriate disciplinary proceedings against the said User.

7. Information Security and Cyber Security

It must be ensured that business information, inclusive of the computing systems is protected from inappropriate access, disclosure or modification. Information, as an asset, should be protected just as any other company asset and therefore to safeguard its value, LTFL *via* this IT Policy has mandated for its employees to go through the IT Policy, understand, accept and practice the rules and regulations that have been defined. It is the Company's policy to:

- Ensure that information is accessible only to those authorized to have access;
- Safeguard the accuracy and completeness of information and processing methods;
- Ensure that authorized users have access to information and associated assets when required;
- Ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information;
- Promote this IT Policy and raise awareness of information security;
- Provide appropriate information security training for the staff;
- Provide a distinct identification number for each information asset and maintain a list of all IT assets of the Company;
- In case the Company stores personal data of its customers, it shall use public key infrastructure to ensure confidentiality of data, access control, data integrity, authentication and nonrepudiation;
- Computer networks and systems outside of the Company is considered as insecure;
- To establish suitable data backup and retention policy

8. Data Backup with Periodic Testing

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility for backing up the information located in shared access servers is the network administrators. It must be borne in mind that not only are hard disks inclined to fail, but also magnetic tapes are quite prone to errors that destroy their contents, so we need to do the restoration testing time to time basis.

- **General Rule**: As daily full backup is happening for all applications.

- **Data Backup in File Servers**: The system management backs up all the information in the file servers through an automated procedure.
- **Data Backup in Database Servers**: The system management backs up all the information in the databases through an automated procedure.
- **Data Backup in Desktop PC and Notebook**: This task is the responsibility of the user to whom the computer has been assigned.

9. Exemptions / Amendments / Delegations

The Board of Directors of the Company shall always have a right to amend / modify / waive any clause / requirement specified under this IT Policy.

****