INFORMATION TECHNOLOGY / INFORMATION SYSTEM POLICY

KRA LEASING LIMITED

Reserve Bank of India vide its circular RBI/DNBS/2016-17/53 (Master Direction DNBS. PPD.No.04/66.15.001/2016-17) of June 8, 2017 has given guidelines for Information Technology Framework for the NBFC sector ("Guidelines"). These Guidelines aim to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers.

IT governance is an integral part of corporate governance of the company, and effective IT governance is the responsibility of the board of directors ("Board") and its executive management.

IT Framework consists of following policies

I. Basic security aspects such as physical/ logical access controls and well-defined password policy;

II. A well-defined user role;

III. A Maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information;

IV. Information Security and Cyber Security;

V. Requirements as regards Mobile Financial Services, social media and Digital Signature Certificates;

VI. System generated reports for Top Management summarizing financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc;

VII. Adequacy to file regulatory returns to RBI;

VIII. A BCP policy duly approved by the Board ensuring regular oversight of the Board by way of periodic reports (at least once every year) ;

IX. Arrangement for backup of data with periodic testing;

Password Policy

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this IT Framework. A strong password must be at least 8 (Eight) characters long.

- It should not contain any of the user's personal information—specifically his/her real name,

- user name, or even company name. It must be very unique from the passwords used previously by the users.

- It should not contain any word spelled completely.

- It should contain characters from the four primary categories i.e. uppercase letters,

- lowercase letters, numbers, and characters. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 30 (Thirty) days. Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorized persons might discover them.

- Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information. Under no circumstances, the users shall use another user's account or password without proper authorization. Under no circumstances, should the user share his/her password(s) with other user(s), unless the said user has obtained from the concerned branch manager/IT head the necessary approval in this regard. In cases where the password(s) is 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 was shared.

Access Controls

Access to the company's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law and as per requirements laid down in this policy.

a. All users must use a unique ID to access company's systems and applications.

b. Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.

c. Remote access to company's systems and applications must use a two-factor authentication where possible

d. System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

Information Security

Information is an asset to all NBFCs and Information Security (IS) refers to the protection of these assets in order to achieve organizational goals. The purpose of IS is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be read or compromised without proper authorization. NBFCs must have a board approved IS Policy with the following basic tenets:

a. **Confidentiality –** Ensuring access to sensitive data to authorized users only.

b. **Integrity –** Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization**.**

c. **Availability –** Ensuring that uninterrupted data is available to users when it is needed.

d. **Authenticity –** For IS it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

The IS Policy must provide for a IS framework with the following basic tenets:

a. **Identification and Classification of Information Assets-**NBFCs shall maintain detailed inventory of Information Asset with distinct and clear identification of the asset**.**

b. **Segregation of functions-** There should be segregation of the duties of the Security Officer/Group (both physical security as well as cyber security) dealing exclusively with information systems security and the Information Technology division which actually implements the computer systems. The information security function should be adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there should be a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

c. **Role based Access Control –** Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), NBFCs shall avoid dependence on one or few persons for a particular job. There should be clear delegation of authority for right to upgrade/change user profiles and permissions and also key business parameters (eg. interest rates) which should be documented.

d. **Personnel Security -** A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose potential threat to systems and data. NBFC should have a process of appropriate check and balance in this regard. Personnel with privileged access like system administrator, cyber security personnel, etc should be subject to rigorous background check and screening.

e. **Physical Security -** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. NBFCs need to create a secured environment for physical security of IS Assets such as secure location of critical data, restricted access to sensitive areas like data center etc.

f. Maker-checker is one of the important principles of authorization in the information systems of financial entities. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information**.**

g. **Incident Management -** The IS Policy should define what constitutes an incident. NBFCs shall develop and implement processes for preventing, detecting, analyzing and responding to information security incidents.

h. Trails- NBFCs shall ensure that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail**.**

i. Public Key Infrastructure (PKI) - NBFCs may increase the usage of PKI to ensure confidentiality of data, access control, data integrity, authentication and nonrepudiation**.**

System generated reports for Top Management

Company has adequate system in preparing quarterly report and get it limited reviewed from its auditor summarizing financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc

Regulatory Returns

Company has adequate system and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorized representatives of the company.

BUSINESS CONTINUITY PLANNING (BCP)

BCP forms a significant part of an organization's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP shall be designed to minimize the operational, financial, legal, reputational and other material consequences arising from a disaster. NBFC should adopt a Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports. The CIO shall be responsible for formulation, review and monitoring of BCP to ensure continued effectiveness. The BCP may have the following salient features**:**

Business Impact Analysis- NBFCs shall first identify critical business verticals, locations and shared resources to come up with the detailed Business Impact Analysis. The process will envisage the impact of any unforeseen natural or man-made disasters on the NBFC's business. The entity shall clearly list the business impact areas in order of priority.

Recovery strategy/ Contingency Plan- NBFCs shall try to fully understand the vulnerabilities associated with interrelationships between various systems, departments and business processes. The BCP should come up with the probabilities of various failure scenarios. Evaluation of various options should be done for recovery and the most cost-effective, practical strategy should be selected to minimize losses in case of a disaster.

NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers**.**

NBFCs shall test the BCP either annually or when significant IT or business changes take place to determine if the entity could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test should be based on 'worst case scenarios. The results along with the gap analysis may be placed before the CIO and the Board. The GAP Analysis along with Board's insight should form the basis for construction of the updated BCP.

Backup Data

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 of backing up the information located in shared access servers is the network administrators. Company also has in place necessary backup sites for their critical business systems and Data centers. These plans are also tested by company on a regular basis. The results along with the gap analysis are placed before the Board.

The Board approves of this IT Framework and has overall charge of the operational functions of Company. The Board is further responsible for timely amending this IT Framework pursuant to its operations and/or any change in the regulations or new regulations issued by the RBI in relation to this IT Framework.