Information Technology Framework

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. NBFCs, pursuant to these Guidelines, are required to conduct a formal gap analysis between their present status and stipulations as set out in the Guidelines and put in place a time-bound action plan to address the gap.

This IT Framework falls within the scope of Section B of the Guidelines i.e. NBFCs with asset size of below INR 500 crores (Indian Rupees Five Hundred Crores only).

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

The NBFC ensures implementation of this IT Framework which, *inter alia*, includes (i) Security aspects; (ii) User Role; (iii) Information Security and Cyber Security; (iv) Business Continuity Planning Policy; (v) Back-up Data.

A. SECURITY ASPECTS

(i) 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. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this IT Framework.

The Complexity Requirements for setting passwords are as follows**:**

- 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. Passwords must not be written down and left in a place 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.

(ii) Access Controls

- Access to the NBFC'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 NBFC policies including but not limited to requirements laid down in this policy.
- Persons or entities with access to the NBFC's electronic information and information systems are accountable for all activities associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by NBFC, irrespective of the medium on which the information resides.
- Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person.
- Requirements:

    a. All users must use a unique ID to access NBFC'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 NBFC 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.

B. INFORMATION SECURITY AND CYBER SECURITY

(i) Information Security:

NBFC has an information security framework with the following principles:

- *Identification and classification of information assets*: NBFC maintains detailed inventory of information asset with distinct and clear identification of the asset.
- *Functions*: The information security function is 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 is a clear segregation of responsibilities relating to system administration, database administration and transaction processing.
- *Role based access control* – Access to information is based on well-defined user roles (system administrator, user manager, application owner.). NBFC has a clear delegation of authority to upgrade/change user profiles and permissions and also key business parameters.
- *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 has a process of appropriate checks and balances to avoid any such threat to its systems and data. Personnel with privileged access like system administrator, cyber security personnel, etc are subject to rigorous background check and screening.
- *Physical Security* - The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. NBFC has created a secured environment for physical security of information assets such as secure location of critical data, restricted access to sensitive areas like data centers etc. and has further obtained adequate insurance to safeguard such data.
- *Maker-checker* – Maker checker is one of the important principles of authorization in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information. NBFC ensures that it complies with this requirement to carry out all its business operations.
- *Trails* - NBFC ensures 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 is recorded in the audit trail.
- *Mobile Financial Services* – NBFC has a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used by NBFC for mobile services ensures confidentiality, integrity and authenticity and provides for end-to-end encryption.
- *Social Media Risks* – NBFC uses social media to market their products and is well equipped in handling social media risks and threats in order to avoid any account takeover or malware distribution. NBFC further ensures proper controls such as encryption and secure connections to mitigate such risks.
- *Digital Signatures* - A Digital signature certificate authenticates entity's identity electronically. NBFC protects the authenticity and integrity of important electronic documents and also for high value fund transfer.

- *Regulatory Returns* – NBFC 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 authorised representatives of NBFC.

(ii) *Cyber Security*

- *NBFC* takes effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions to respond / recover / contain the fall out. Among other things, NBFC takes necessary preventive and corrective measures in addressing various types of cyber threats which includes denial of service, distributed denial of services (DDoS), ransom- ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds and password related frauds.
- NBFC realises that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. NBFC ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats. Further, it also proactively promotes, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and ensures appropriate action to support their synchronised implementation and testing.

(iii) ***Confidentiality***

- NBFC, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.
- Access to customer information by employees of the service provider to NBFC is on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.
- NBFC further ensures that the service provider isolates and clearly identifies NBFC's customer information, documents, records and assets to protect the confidentiality of the information. NBFC has strong safeguards in place so that there is no comingling of information / documents, records and assets.
- NBFC ensures that it immediately notifies RBI in the event of any breach of security and leakage of confidential customer related information.

C. BACK-UP OF DATA 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 of backing up the information located in shared access servers is the network administrators'.
- Restoration testing on a time to time basis is done as both hard disks and magnetic tapes are prone to errors. As a general rule, daily full backup happens for all critical business application and a complete weekly full backup is carried out including file servers/old data kept on servers.

The Board approves of this IT Framework and has overall charge of the operational functions of NBFC. 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.