INFORMATION TECHNOLOGY POLICY

OF TAMIL NADU URBAN FINANCE AND INFRASTRUCTURE DEVELOPMENT CORPORATION LIMITED

1. Preamble

1.1 The Reserve Bank of India ("RBI") had, vide its Notification No RBI/DNBS/2016-17/53 Master Direction DNBS.PPD.No.04/66.15.001/2016-17 Dated June 8, 2017 issued "Master Direction - Information Technology Framework for the NBFC Sector", mandated every Regulated NBFC may start with developing basic IT systems mainly for maintaining the database. NBFCs with asset size below ₹ 500 crores shall have a Board approved Information Technology Policy/Information System Policy (hereinafter referred to as the "Policy").

1.2 Tamil Nadu Urban Finance and Infrastructure Development Corporation Limited (the "Company"), being a Government company as defined under clause (45) of Section 2 of the Companies Act, 2013 (Act 18 of 2013) and a non-banking financial company registered with the Reserve Bank of India under the provisions of RBI Act, 1934 and is accordingly required to put such a Policy in place.

1.3 This policy is to be approved by the Board of Directors at its next meeting to be held on September 6, 2021.

2. Background

2.1 The evolution of computer networks has made the sharing of information ever more prevalent. Information is now exchanged at the rate of trillions of bytes per millisecond, daily numbers that might extend beyond comprehension or available nomenclature. Information Technology Policy is a set of measures issued by NBFCs to ensure that all information technology users within the domain of the Company or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network.

2.2 Customer Information, organizational information, supporting IT systems, processes, and people that are generating, storing, and retrieving information are important assets of the NBFC. The availability, integrity, and confidentiality of information are essential in building and maintaining our competitive edge, cash flow, profitability, legal compliance, and respected company image.

2.3 The Information Security Policy provides an integrated set of protection measures that must be uniformly applied across NBFC to ensure a secure operating environment for its business operations.

3. Scope

3.1 This policy applies to all employees, contractors, service providers, Interns/Trainees working in the NBFC. Third-party service providers providing hosting services or wherein data is held outside NBFC premises, shall also comply with this policy.

3.2 Scope of this Information Technology Policy is the Information stored, communicated, and processed within NBFC and NBFC's data across outsourced service provider's locations.

4. Objectives

4.1 The objective of the Information Technology Policy is to provide NBFC, an approach to managing information risks and directives for the protection of information assets to all units, and those contracted to provide services.

4.2 The objectives of this Policy are:
4.2.1 Developing Information Technology System for maintaining the database.
4.2.2 To frame Information Technology Standards and measures for Company in order to comply with above said Master Direction.
4.2.3 To ensure that each person appointed or already appointed understands the Information Technology Policy and their obligation to meet its requirement.

5. Definitions

(a) "Bank" means the Reserve Bank of India constituted under section 3 of the Reserve Bank of India Act, 1934

(b) “Board” means Board of Directors of the Company for the time in force;

(c) “Company” or “TUFIDCO” means “Tamil Nadu Urban Finance and Infrastructure Development Corporation Limited”;

(d) “Policy” means the Information Technology Policy.

6. Criteria for Information Technology Policy

The guidelines in respect of Information Technology Policy in the Company broadly includes the following:

6.1 Basic security aspects such as physical/ logical access controls and a well-defined password policy

6.1.1 Access Controls

The confidentiality, integrity, and availability of information can be impaired through Physical /Logical Access Controls and damage or destruction to physical components. NBFC requires creating a protected environment for the physical security of Information Security Assets such as the secure location of critical data, restricted access to sensitive areas like a data centre.

6.1.2 Password

6.1.2.1 The Company is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change all Application software in NBFC.
6.1.2.2 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.
6.1.2.3 The Complexity Requirements for setting passwords are as follows:
6.1.2.3.1 A strong password must be at least 8 (Eight) characters long.
6.1.2.3.2 It should not contain any of the user’s personal information—specifically his/her real name, user name, or even company name.
6.1.2.3.3 It must be very unique from the passwords used previously by the users.

6.1.2.3.4 It should not contain any word spelled completely.
6.1.2.3.5 It should contain characters from the four primary categories i.e., uppercase letters, lowercase letters, numbers, and characters
6.1.2.3.6 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.
6.1.2.3.7 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.
6.1.2.3.8 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.
6.1.2.3.9 Under no circumstances, the users shall use another user's account or password without proper authorization.
6.1.2.3.10 Under no circumstances, should the user share his/her password(s) with other user(s), unless the said user has obtained from the concerned section head/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.

6.2 A well-defined user role:
Access to information should be based on well-defined user roles (system administrator, user manager, application owner, etc.), NBFC shall avoid dependence on one or few persons for a particular job. There should be a clear delegation of authority for the right to upgrade/change user-profiles and permissions and also key business parameters (e.g., interest rates) which should be documented.

6.3 Implementation of the Maker-checker concept to reduce the risk of errors and misuse and to ensure reliability of data/information:
Maker-checker is one of the important principles of authorization in the information systems of financial entities. It is to reduce the risk of error and misuse and to ensure the reliability of data/information. 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 the reliability of the information.

6.4 Provisions pertaining to Information Security and Cyber Security:
6.4.1.1 Incident management is required and needs to be established to ensure a quick, effective, and orderly response to security incidents. Such a policy would vary in scope depending on the sensitivity and size of the information systems being managed. A companywide incident management policy has been established for all systems.
6.4.1.2 Information is an asset, and Information Security (IS) refers to the protection of these assets 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.
6.4.1.3 This Information Security Policy addresses the information security requirements of:
6.4.1.3.1 Confidentiality: Protecting sensitive information from disclosure to unauthorized individuals or systems;
6.4.1.3.2 Integrity: Safeguarding the accuracy, completeness, and timeliness of information;
6.4.1.3.3 Availability: Ensuring that information and vital services are accessible to authorized users when required

6.4.1.4 Other principles and security requirements such as Authenticity, Non-repudiation, Identification, Authorization, Accountability, and audit ability are also addressed in this policy.

6.4.2 Cyber-Security Awareness Among Stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. NBFCs should proactively promote, among their customers, vendors, service providers, and other relevant stakeholders an understanding of their cyber resilience objectives and require and ensure the appropriate action to support their synchronized implementation and testing.

6.5 Requirements as regards Mobile Financial Services, Social Media and Digital Signature Certificates:

6.5.1 Mobile Financial Services

NBFCs that are already using or intending to use Mobile Financial Services should develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption.

6.5.2 Social Media Risks

NBFCs using Social Media to market their products should be well equipped in handling social media risks and threats. As Social Media is vulnerable to account takeovers and malware distribution, proper controls, such as encryption and secure connections, should be prevalent to mitigate such risks.

6.5.3 Digital Signatures

A Digital Signature Certificate authenticates entity's identity electronically. It also provides a high level of security for online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. NBFCs may consider use of Digital signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.

6.6 Creation of system generated reports for Top Management summarising financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc.:

6.6.1 IT function of an NBFC should support a robust and comprehensive Management Information System (MIS) in respect of various business functions as per the needs of the business. A good MIS should take care of information needs at all levels in the business including top management.

6.6.2 NBFC should put in place MIS that assists the Top Management as well as the business heads in decision making and also to maintain oversight over operations of various business verticals. With robust IT systems in place, the NBFC should have the following as part of an effective system generated MIS (indicative list)

6.6.2.1 A dashboard for the Top Management summarising financial position vis-à-vis targets. It may include information on-trend on returns on assets across categories, major growth business segments, movement of net-worth, etc.

6.6.2.2 The system enabled identification and classification of Special Mention Accounts and Non Performing Assets, as well as generation of MIS, reports in this regard.

6.6.2.3 The MIS should facilitate the pricing of products, especially large ticket loans.

6.6.2.4 The MIS should capture regulatory requirements and compliance.

6.6.2.5 Financial Reports including operating and non-operating revenues and expenses, cost-benefit analysis of segments/verticals, cost of funds, etc. (also regulatory compliance at transaction level)

6.7 Adequacy to file regulatory returns to the RBI (COSMOS Returns):
NBFCs' management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during compliance. Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance should be delineated in the framework.

6.8 A Business Continuity Planning (BCP) policy duly approved by the Board ensuring regular oversight of the Board by way of periodic reports (at least once every year):
6.8.1 NBFC should undertake a comprehensive risk assessment of their IT systems at least every year. The assessment should analyze the threats and vulnerabilities to the information technology assets of the NBFC and its existing security controls and processes. The outcome of the exercise should be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks.
6.8.2 The policy should be Board Approved and it shall be reviewed every year or at the time of any major change in the existing IT environment affecting policy and procedures and placed to Board for approval.

6.9 Arrangement for backup of data with periodic testing:
All of the records are to be maintained within the Company's centralized electronic record software database, A backup of all of the data with periodic testing. shall take periodically for the preservation of Data.

7. Gap Analysis

NBFCs are required to conduct a formal gap analysis between their current framework and the stipulations laid out in the Directions and put in place a time-bound action plan to address the gaps, if any, and comply with the Directions.

8. Review

IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures and placed to Board for approval.