SUNSHINE CAPITAL LIMITED.

GUIDELINES ON INFORMATION TECHNOLOGY (IT) POLICY

Policy Governance

Frequency of Review	**Annual**
Framed & Last reviewed & Amended on	**15/07/2022**
Approved By	**Board of Directors**

INFORMATION TECHNOLOGY POLICY

I. INTRODUCTION

SUNSHINE CAPITAL LIMITED. ('the Company'/ **SCL**) recognizes its role as a corporate citizen and endeavors to adopt the best business practices and the highest standards through transparency in business ethics, accountability to its customers, government and others. The Company's activities are carried out in accordance with good business practices and the Company is constantly striving to better them and adopt the best practices.

The Company is a registered Non-Deposit taking Systemically Important Non-Banking Financial Company ("NBFC-ND-SI") and has received a Certificate of Registration from RBI. The Company's philosophy on Information Technology policy that it's era of technology, Information Technology (IT) aids plenty of resources to enhance the credit system of the country and through the information technology its ease in doing the business in ethical and transparent way.

II. OBJECTIVE OF GUIDELINES

In the era of technology, Information Technology (IT) aids plenty of resources to enhance the credit system of the country. Over the years, the Non-Banking Finance Company (NBFC) sector has grown in size and complexity. As the NBFC industry matures and achieves scale, its Information Technology /Information Security (IT/IS) framework, Business continuity planning (BCP), Disaster Recovery (DR) Management, IT audit, etc. must also be benchmarked to best practices.

To enhance the safety, security, efficiency in processes leading to benefits for NBFCs and their customers. The focus of the proposed IT framework is on IT Governance, IT Policy, Information & Cyber Security, IT Operations, IS Audit, Business Continuity Planning and IT Services Outsourcing, the Reserve Bank of India (RBI) has come up with the ***Master Direction – Information Technology Framework for the NBFC Sector ("Directions") vide its notification no. Master Direction DNBS.PPD.No.04/66.15.001/2016-17 dated June 08, 2017.*** (Amended time to time). These Directions have not just laid down a mere statement of good intentions but are largely focusing on implementing several operational requirements.

III. APPLICABILITY

1. Directions applicable to all NBFCs with asset size above Rs. 500 Crore (Considered systemically important) are provided.
2. Directions for NBFCs with asset size below Rs. 500 Crore.

IV. TIMELINES FOR COMPLIANCE

NBFCs- Systemically Important shall comply with the Master Directions by June 30, 2018 and other NBFCs (asset size below Rs. 500 Crore) shall comply by September 30, 2018. NBFCs may have already implemented or may be implementing some of the requirements indicated in the Directions. Therefore, the NBFCs are now required to conduct a formal gap analysis between their current status and stipulations as laid out in the Directions and put in place a time-bound action plan to address the gap and comply with the guidelines laid therein. Such an analysis may be submitted to the Board of the company within six months of the issuance of these directions.

V. ACCORDINGLY ("THE COMPANY") HAS FRAMED A POLICY ON INFORMATION TECHNOLOGY AS UNDER:

The focus of the proposed IT framework is on **IT Governance, IT Policy, Information & Cyber Security, IT Operations, IS Audit, Business Continuity Planning and IT Services Outsourcing.** The broad actions have been undertaken by the company NBFC-SI along with the guidelines issued in this regard has been tabulated below for an easy reference.

IT Governance		
Who shall be responsible for the implementation of an effective IT Governance	**Board of Directors and Executive Management**	Well-defined roles and responsibilities to enable effective project control
Who are the **IT Governance Stakeholders**?	a. Board of Directors, b. IT Strategy Committees, c. CEOs, d. Business Executives, e. Chief Information Officers f. Chief Technology Officers g. IT Steering committees (operating at an executive level and focusing on priority setting, resource allocation and project tracking), h. Chief Risk Officer and Risk Committees	
Action Points	Formation of an **IT Strategy Committee**	**Chairman of the Committee**: An independent director **Other Members**: CIO & CTO **Frequency of Meeting**: An appropriate frequency with maximum gap of 6 months between two meetings **Role of the Committee**: i. Providing input to other Board committees and Senior Management. ii. Carrying out review and amending the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance iii. Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place; Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business;

		Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable; Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources; Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.

IT POLICY		
Action Points	Formulating a Board approved **IT policy**	The policy shall be in line with the organizational objectives
	Develop an **IT organizational structure**	The structure shall be commensurate with the size, scale and nature of business activities carried out by the NBFC
	Designate a senior executive as the Chief Information Officer (CIO) or in-Charge of IT operations	The responsibility of such officer shall be to ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management and IT resource management.
	Formulate **periodic assessment** of the IT training requirements	To ensure **technical competence** at senior/middle level management and to ensure that sufficient, competent and capable human resources are available
	Migrate to the IPv6 platform as per National Telecom Policy issued by the Government of India in 2012[1]	

INFORMATION AND CYBER SECURITY		
Action Points	Formulating a board approved **IS Policy**	The IS Policy shall be based on the following principles: i. **Confidentiality** – Ensuring access to sensitive data to authorized users only. ii. **Integrity** – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization. iii. **Availability** – Ensuring that uninterrupted data is available to users when it is needed. iv. **Authenticity** – For IS it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.
	IS framework must be provided in the IS Policy	The IS framework shall be based on the following principles: i. **Identification and Classification of Information Assets.** ii. **Segregation of functions and responsibilities** relating to system administration, database administration and transaction processing. iii. **Role based Access Control by** clear **delegation of authority** for right to upgrade/change user profiles and permissions and also key business parameters (e.g. interest rates) which should be documented. iv. **Personnel** with privileged access like system administrator, cyber security personnel, etc should be subject to **rigorous background check.** 1. **Physical Security by** creating a secured environment for physical security of IS Assets such as secure location of critical data, restricted access.

		2. For each transaction, there must be at least two individuals (**Maker-checker** is one of the important principles of authorization in the information systems of financial entities) necessary for its completion as this will reduce the risk of error and will ensure reliability of information. 3. **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. 4. **Trails**- NBFCs shall ensure that audit trails exist for IT assets satisfying its business requirements. If an employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail. 5. **Public Key Infrastructure (PKI)** – NBFCs may increase the usage of PKI to ensure confidentiality of data, access control, data integrity, authentication and non repudiation.
	Formulating a board approved **cyber-security policy**	The policy shall elucidate the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.
	Vulnerability Management	Devise a **strategy for managing and eliminating vulnerabilities** and such strategy may clearly be communicated in the Cyber Security policy.
	Cyber security preparedness indicators	a. Development of indicators to assess the level of risk/preparedness b. Spreading awareness among the stakeholders including employees
	A **Cyber Crisis Management Plan (CCMP)**should be immediately evolved and should be a part of the overall Board approved strategy	The CCMP shall be addressing the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment
	Take effective measures to be well prepared to: 1. prevent cyber-attacks 2. promptly detect any cyber-intrusions 3. face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.	Take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, 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, password related frauds, etc
	Sharing of information on cyber-security incidents with RBI	Report all types of unusual security incidents as specified in CSIR Form of Annex I (both the successful as well as the attempted incidents which did not fructify) to the DNBS Central Office, Mumbai.
	Cyber-security awareness among stakeholders / Top Management / Board	Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarization may be organized.
		Promote, among the customers, vendors, service providers and other relevant stakeholders an understanding of the cyber resilience objectives, and require and ensure appropriate action to support the synchronized implementation and testing.

	Digital Signatures	Consider use of Digital signatures to **protect the authenticity and integrity of important electronic documents** and also for high value fund transfer.
	IT Risk Assessment	Undertake a comprehensive **risk assessment of IT systems at least on a yearly basis** and bring to the notice of the Chief Risk Officer (CRO), CIO and the Board and serve as an input for Information Security auditors
		Finding out the risks present and determining the appropriate level of controls necessary for appropriate mitigation of risks
	Mobile Financial Services	Technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption
	Social Media Risks	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.
	Training	Conduct an initial and ongoing training and information security awareness programmed
IT Operations		
Action Points	Establish and monitor policies for risk management	The Board or Senior Management should take into consideration the risk associated with existing and planned IT operations and the risk tolerance.
	Identify **system deficiencies and defects** at the system design, development and testing phases	To ensure that while implementing IT projects there are no systems failure because of poor system design and implementation, as well as inadequate testing.
	Establish a **steering committee**	The committee shall be consisting of **business owners, the development team and other stakeholders** to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.
	Develop a Board approved **Change Management Policy** and senior management to ensure that the policy is being followed on an ongoing basis	The Policy must encompass the following: 1. prioritizing and responding to change proposals from business, 2. cost benefit analysis of the changes proposed, 3. assessing risks associated with the changes proposed, 4. Change implementation, monitoring and reporting.
	Put in place a **good MIS**	The MIS shall take care of information at all levels in the business including top management and assists the Top Management as well as the business heads in decision making and also to maintain an oversight over operations of various business verticals.
	System driven regulatory/ supervisory returns	There should be seamless integration between MIS system of the NBFC and reporting under COSMOS.
IS Audit		
Action Points	Formulate a **Policy for Information System Audit (IS Audit)**	IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.

	Adopt an **IS Audit framework** duly approved by the Board	The framework shall lay down the following:- a) Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance should be clearly delineated in the framework. b) The framework may provide for an audit-mode access for auditors/ inspecting/ regulatory authorities. c) The framework should clearly prescribe the reporting framework Guidance issued by Professional bodies like ISACA, IIA, ICAI in this regard shall be referred. For instance, ICAI has published "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment".
	Composition of **Audit Committee**	An adequately skilled personnel should be there in Audit Committee who can **understand the results of the IS Audit**
	Coverage of IS Audit	Due importance shall be given to compliance of all the applicable legal and statutory requirements
	Conduct of IS Audit	By an **internal team** of the NBFC or an **outside agency** having enough expertise in area of IT/IS audit
	Periodicity	The periodicity of IS audit should ideally be based on the size and operations of the NBFC but **may be conducted at least once in a year** and be undertaken preferably prior to the statutory audit
	Reporting	As provided in the IS framework, either to the **Board or a Committee of the Board** viz. Audit Committee of the Board
	Compliance	NBFCs' management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit
	Computer-Assisted Audit Techniques (CAATs)	To adopt a proper mix of manual techniques and CAATs for conducting IS Audit
Business Continuity Planning		
Action Points	Formulate and adopt a Board approved **BCP Policy**	To minimize the operational, financial, legal, reputational and other material consequences arising from a disaster
	Salient features of the BCP	a. **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. b. **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.
	Functioning of BCP	a. To be monitored by the Board by way of periodic reports. b. CIO shall be responsible for formulation, review and monitoring of BCP to ensure continued effectiveness
	Review of 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
	Put in place necessary **backup sites** for critical business systems and Data centers	

IT Services Outsourcing		
Action Points	**Outsourcing of IT related business**	The terms and conditions governing the contract between the NBFC and the Outsourcing service provider should be carefully defined in **written agreements and vetted by NBFC's legal counsel** on the legal effect and enforceability
To be Noted	**Provisions of contractual agreement**	**a) Monitoring and Oversight:** Provide for **continuous monitoring and assessment by the NBFC** of the service provider so that any necessary corrective measure can be taken immediately. Outsourcing service provider should have adequate systems and procedures in place to ensure protection of data/application outsourced. **b) Access to books and records / Audit and Inspection:** This would include: a) Ensure that the NBFC has the ability to **access all books, records and information relevant to the outsourced activity** available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the NBFC based on approved requests. b) Provide the NBFC with the **right to conduct audits on the service provider** whether by its internal or external auditors, or by external specialists audit or review reports and findings made on the service provider in conjunction with the services performed for the NBFC. c) The contractual agreement may include clauses to allow the **Reserve Bank of India or persons authorized by it to access the NBFC's documents**, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats.
	Responsibility for outsourcing	**Board and senior management** are ultimately responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships.
	Role of IT Strategy committee in respect of outsourced operations	1. Instituting an appropriate governance mechanism for outsourced processes, comprising of risk based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner; 2. Defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing; 3. Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements; 4. Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements; 5. Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board; 6. Periodically reviewing the effectiveness of policies and procedures;

SUNSHINE CAPITAL LIMITED New Delhi

		7. Communicating significant risks in outsourcing to the NBFC's Board on a periodic basis; 8. Ensuring an independent review and audit in accordance with approved policies and procedures; 9. Ensuring that contingency plans have been developed and tested adequately; 10. NBFC should ensure that the business continuity preparedness is not adversely compromised on account of outsourcing. NBFCs are expected to adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

For SUNSHINE CAPITAL LIMITED

DIRECTOR

THE END