IBL FINANCE LIMITED

REGISTERED OFFICE: Shop – 151, Silver Stone Arcade, Nr. Kanthariya Hanuman Temple, OP-34/A+B+C+D,FP-50, Singanpore Causeway Road, Surat – 395004, Gujarat.

Outsourcing Policy

1. Preamble

This Outsourcing Policy ("Policy") of IBL Finance Limited ("Company") has been formulated and adopted by the Company to safeguard the interest of the Company and its Customers by adopting sound and responsive management practices through due diligence and management of risks arising from Outsourcing of Business Functions. The Policy is based on the RBI Master Directions titled "Non-Banking Financial Company - Non-Systemically Important Non-Deposit taking Company (Reserve Bank) Directions, 2016" and is applicable to all Outsourcing arrangements entered into by the Company with Service Provider(s) located in India as well as outside India.

2. Objective

The Policy incorporates the criteria for selection of Service Providers, materiality of services Outsourced, delegation of authority depending on risks and materiality, and systems to monitor and review the operations of the activities outsourced. The Policy shall apply to all Outsourcing to Service Provider(s) and *mutatis mutandis* to activities subcontracted by the Service Providers.

The Policy also incorporates Code of Conduct ('Code') designed to guide the conduct of DSAs/DMAs/DRAs engaged by the Company. The Code enumerates guidelines for the agents dealing directly with the Customers. The employees of the Company directly dealing with the Customers, if any shall also comply with the Code.

3. Definitions

Unless otherwise defined or apparent from context, the following terms shall have the meaning as assigned herein below, and cognate expressions shall be construed accordingly:

Board	Shall mean the Board of Directors of the Company;
Business Function	Shall mean one or more functions, customarily or by statute required or expected to be performed by the Company, excluding any activities, tasks or functions which may, for the reason of business expediency, costs, efficiency, expertise or otherwise typically be handled by external agencies, engaged by the Company and working for or for the benefit of the Company;
Code	The Code of Conduct for the Direct Selling Agents (DSAs) / Direct Marketing Agents (DMAs) / Debt Recovery Agents (DRAs), as provided in Annexure to this Policy.
Company	Shall mean IBL Finance Limited;

Confidential Information	Includes but is not limited to all proprietary and confidential information of the Company or its holding company, subsidiaries, affiliates, or licensees, including without limitation all information, in any form, tangible or maintained in electronic form, including without limitation applications, charts, data, documents, models, worksheets, formulae, policies, templates, forms, instruments, papers or statements, regarding the Company or its holding company, subsidiaries, affiliates, or licensees; also includes information on the Customers of the Company or the Customers of any of its subsidiaries, affiliates, or licensees, including without limitation the accounts, account numbers, names, addresses or any other personal identifiers of such Customers, or any information derived therefrom;
Compliance Officer	Shall mean such person as authorized by the Board to ensure compliance with the RBI regulations;
Customer	Shall mean any existing or prospective customers of the Company;
Direct Marketing Agents (DMA)	The persons employed for marketing, promoting, and advertising the Company's Financial Products through which they endorse the Company's brand.
Debt Recovery Agent (DRA)	The persons employed for the purpose of collecting outstanding dues from Customers who are delinquent or have defaulted on their repayment of the loan or credit facility.
Direct Selling Agents (DSA)	The persons employed for the purpose of selling the Financial Products of the Company.
Functional Department	Shall mean the specific department of the Company performing and undertaking any Business Function within the organization;
Functional Head	Shall mean the head of a Functional Department;
Financial Product	A loan or other financial product or service provided or proposed to be provided by the Company.
Grievance Redressal Machinery	Shall mean the Grievance Redressal Machinery constituted by the Company;
Material Outsourcing	Shall mean such Outsourcing activities that have been identified and classified as such in accordance with para 7.1 of the Policy;
Non-Material Outsourcing	Shall mean such Outsourcing activities other than Material Outsourcing;
Outsourcing	Shall refer to the Company's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform Business Functions pertaining to the business of financial services, on a continuing basis, including agreements for a limited period, that would normally be undertaken by the Company itself, now or in the future;
Policy	Shall mean this Outsourcing Policy, as amended from time to time;
Prescribed Time	The time period between 07:00 a.m. to 07:00 p.m.
RBI Directions	Non-Banking Financial Company - Non-Systemically Important Non-Deposit taking Company (Reserve Bank) Directions, 2016

Senior Management	Shall mean personnel of the Company who are members of its core management team excluding the Board, comprising all members of the Executive Committee of the Company, including the Functional Heads;
Service Provider	Shall mean any person or entity appointed or proposed to be appointed by the Company to carry out the Outsourcing activities that may either be a member of the group/ conglomerate to which the Company belongs, or an unrelated party.

4. Role of the Board of the Company

4.1. The Board, as the apex supervisory organ of the Company, shall have the overall responsibility to settle the Company's approach towards Outsourcing, especially any Material Outsourcing, the administrative framework for the same, and evaluation and mitigation of any risks inherent in Material Outsourcing.

4.2. The Board may, from time to time, review this Policy and seek reports on the implementation hereof or exceptions to the same.

4.3. The Board shall undertake regular review of Outsourcing strategies and arrangements for their continued relevance, safety and soundness.

4.4. The Board shall have the right to ratify any deviations from the Policy.

5. Responsibilities of Senior Management

5.1 Approve any Outsourcing within a Business Function.

5.2 Continue to monitor all Outsourcing activities, and in particular, identify the Functional Heads relevant to any Outsourcing.

5.3 Periodically evaluate risks and materiality of all Outsourcing arrangements and communicate information about Material Outsourcing to the Board.

5.4 Ensure contingency plans, based on realistic and probable disruptive scenarios, are in place and tested.

6. Outsourcing of Services

For the purposes of this Policy, Outsourcing activities shall refer to Outsourcing of financial or related services only. Any kind of technology-related issues and activities not related to financial services, such as usage of courier, housekeeping and janitorial services, security of the premises, movement and archiving of records, etc. are not covered under the purview of this Policy.

6.1 Activities which cannot be Outsourced

Core management functions including Internal Audit, Strategic and Compliance functions and decision-making functions such as determining compliance with KYC norms for opening customer accounts, according sanction for loans, and management of investment portfolio shall not be Outsourced by the Company to any outside entity. However, the same can be outsourced to entities in the same group/ conglomerate in which the Company belongs in the manner laid down herein below in Para 9 and in compliance with the RBI Directions.

6.2 Activities which can be Outsourced

Financial services that can be Outsourced by the Company may include loan application processing, loan origination, document processing, marketing and research, supervision of loans, recovery of loans, data processing, and back office related activities.

7. Aspects Related to Outsourcing

7.1 Criteria for Classification as Material

The Functional Head would identify and classify each of the activities Outsourced/proposed to be Outsourced as "Material Outsourcing" and "Non- Material Outsourcing" based on the below mentioned illustrative parameters:

7.1.1.1. The extent of reliance of Company on Service Provider(s) to perform the key financial functions such as loan applications processing, verifications, approvals, recovery of loans, etc., on a continuous basis;

7.1.1.2. The exposure of the Company to a variety of risks, as specified in para 7.2, with respect to the Outsourced activity;

7.1.1.3. The nature of the activity Outsourced i.e.

(a) whether the activity is such that the performance of the Service Provider can significantly impact, directly or indirectly, the earnings, solvency, liquidity, funding capital and risk profile of the Company;

(b) whether the activity is such that failure on the part of the Service Provider to perform the service efficiently as per contract is likely to significantly impact the Company's reputation and brand value;

7.1.1.4. The potential of the Outsourced activity, to significantly impact business operations, reputation and stability of the Company, in case it is disrupted;

7.1.1.5. The impact of the Outsourced activity on data privacy and security. For instance where access to any Confidential Information has to be extended to employees/representatives of the Service Provider;

7.1.1.6. The cost of Outsourcing an activity as a proportion to the total operating costs of the Company. The cost shall be compared with operating costs of the previous financial year and it shall be determined whether such cost is more than 10 %.

7.1.1.7. Involvement and significant sharing of Confidential Information in the arrangement.

In case the activity Outsourced satisfies any of the above criteria, or similar criteria indicating the materiality of the activity to the business model of the Company, the activity Outsourced would be treated as "**Material Outsourcing**".

The Functional Head shall be responsible for identifying any Outsourcing proposed, and determine whether the same is Material Outsourcing or Non-material Outsourcing.

The Functional Head shall ensure that any Material Outsourcing proposed is put for the approval of the Compliance Officer or such other person authorized by the Board.

The Board and Senior Management must undertake a periodic review of their Outsourced processes to identify new Outsourcing risks as they arise.

7.2 Categorization of risk

Outsourcing of financial services exposes the Company to a number of risks, as specified in the RBI Directions. These are more specifically mentioned herein below, and need to be evaluated and effectively managed and mitigated.

7.2.1 **Strategic Risk** – Where the Service Provider conducts business on its own behalf, inconsistent with the overall strategic goals of the Company.

7.2.2 **Reputation Risk** – Where the service provided is poor and customer interaction is not consistent with the overall standards expected of the Company.

7.2.3 **Compliance Risk** – Where privacy, consumer and prudential laws are not adequately complied with by the Service Provider.

7.2.4 **Operational Risk** – Where there is a technology failure, fraud, or inadequate financial capacity to fulfill obligations and/ or to provide remedies.

7.2.5 **Legal Risk** – Where the Company is subjected to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the Service Provider.

7.2.6 **Exit Strategy Risk** – Where the Company is over-reliant on one Service Provider, such that the loss of relevant skills in the Company itself is preventing it from bringing the activity back in-house and where Company has entered into contracts that make speedy exits prohibitively expensive.

7.2.7 **Counterparty Risk** – Where there is inappropriate underwriting or credit assessments.

7.2.8 **Contractual Risk** – Where the Company may not have the ability to enforce the contract.

7.2.9 **Concentration and Systemic Risk** – Where the overall industry has considerable exposure to one Service Provider and hence, the Company may lack control over the Service Provider.

7.2.10 **Country Risk** – Where there is an unstable political, social or legal climate, thereby creating added risk.

7.3 Outsourcing Procedure

It is necessary to enable sound and responsive risk management practices for effective oversight, due diligence and management of risks arising from Outsourcing activities. All of the Outsourcing arrangements entered into by the Company must be in conformity with the standards laid down in the RBI Directions and shall be subject to the following:

7.3.1 General Conditions

(a) When Outsourcing a financial activity, the Company shall consider all relevant laws, regulations, guidelines and conditions of approval, licensing or registration.

(b) The Company shall retain ultimate control of the Outsourced activity, as Outsourcing of any activity by the Company does not diminish its obligations, and those of its Board and Senior Management, who have responsibility for the Outsourced activity.

(c) The Outsourcing of activities to Service Providers shall in no manner release the Company or the Board or Senior Management of the Company from any obligations towards its Customers, regulatory authorities or any other stakeholder, arising from the provisions of RBI Directions or otherwise.

(d) The Company shall remain responsible for the actions of its Service Provider(s) and the security of Confidential Information pertaining to the Customers that is available with the Service Provider.

(e) Outsourcing arrangements shall neither diminish the Company's ability to fulfill its obligations to Customers and RBI nor impede effective supervision by RBI. The Company shall, therefore, ensure that the Service Provider employs the same high standard of care

in performing the services as would be employed by the Company, if the activities were conducted within the Company and not Outsourced.

(f) The Company shall ensure that the Service Provider does not impede or interfere with the ability of the Company to effectively oversee and manage its activities nor does it impede the RBI in carrying out its supervisory functions and objectives. Therefore, the right of the Company and the RBI to access all books, records and information available with the Service Provider must remain protected.

(g) Outsourcing arrangements shall not affect the rights of the Customer against the Company, including the ability of the Customer to obtain redress as applicable under relevant laws.

7.3.2 Selection of Service Provider

The identification and selection of the Service Provider shall be in the manner provided under the RBI Directions and the Company shall also evaluate the capability and competence of Service Provider in the manner provided in RBI Directions. While Outsourcing or renewing a contract of an activity with a Service Provider, the Company shall take into consideration the following:

(a) The Service Provider, other than a group company, is not owned or controlled by any director of the Company or their relatives, having the same meaning as assigned under Section 2 (77) of the Companies Act, 2013

(b) The capability of the Service Provider to comply with obligations under the Outsourcing agreement such as:
   i) Qualitative, quantitative, financial, operational and reputational factors;
   ii) Compatibility with their own systems;
   iii) Ability to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures;
   iv) Carrying out a periodic test of the business continuity and recovery plan;
   v) Ability to isolate the Company's information, documents and records, and other assets;
   vi) Strong safeguards to ensure that there is no commingling of information, documents, records, and assets.

(c) The concerned Functional Department of the Company shall remain responsible for understanding and monitoring the control environment of Service Providers that have access to the Company's systems, records, or resources.

7.3.3 Due Diligence

(a) Before entering into a fresh Outsourcing arrangement or renewing an Outsourcing arrangement, the concerned Functional Department must perform due diligence to assess the capability of the Service Provider to comply with obligations under the Outsourcing agreement. In order to examine the capability on the above points an evaluation shall be conducted of all available information about the Service Provider, including but not limited to:
   i) Past experience and competence to implement and support the proposed activity over the contracted period;
   ii) Financial soundness and ability to service commitments even under adverse conditions;
   iii) Business reputation, culture, and compliance with applicable laws;
   iv) Complaints and outstanding or potential litigation;

v) Standards of performance including in the area of Customer service;
vi) Security and internal control, audit coverage, reporting and monitoring environment, and Business continuity management;
vii) Technical abilities, data privacy policies and storage systems, fairness in conduct with borrowers and ability to comply with regulations & statutes;
viii) Business continuity arrangements and recovery plans;
ix) Due diligence of employees, representatives and sub-service providers, as well as employee training;
x) Wherever possible, the Company shall obtain independent reviews and market feedback on the Service Provider to supplement its own findings.

It must be ensured that information used for due diligence is not more than 12 months old.

(b) The Company shall avoid undue concentration of Outsourcing arrangements with a single Service Provider.

(c) While selecting a Service Provider, the concerned Functional Department shall identify Business Functions to be Outsourced along with necessary controls. Due diligence undertaken during the selection process shall be documented and re-performed periodically as part of the monitoring and control processes of Outsourcing.

(d) The identification of risk and management of risk with respect to the activities Outsourced shall be carried out by the Company, as a whole, in the manner provided in the RBI Directions. The concerned Functional Department that decides to outsource a financial activity /service shall perform a risk evaluation prior to entering into an Outsourcing agreement and the same shall be reviewed periodically in the light of known and expected changes, as part of the strategic planning or review processes.

(e) The framework for risk evaluation shall include the following steps:
(i) Identification of the role of Outsourcing in the overall business strategy and objectives, and inter-linkages with the Company's strategic goals;
(ii) Comprehensive due diligence on the nature, scope, and complexity of the Outsourcing to identify the key risks and risk mitigation strategies;
(iii) Analysis of the impact of such an arrangement on the overall risk profile of the Company, and whether adequate internal expertise and resources exist to mitigate the risks identified;
(iv) Analysis of the risk-return on the potential benefits of Outsourcing and the vulnerabilities that may arise.

(f) All Outsourced information systems and operations may be subject to risk management and security and privacy policies that meet the Company's own standards and also those mentioned in the RBI Directions.

7.3.4 Monitoring and Control of Outsourced Activities

The Company shall continue to monitor and control the Outsourced activities in the manner provided in the RBI Directions. In order to mitigate the risk of unexpected termination of the Outsourcing agreement or liquidation of the Service Provider and in order to establish a structure for management and control of Outsourcing, the concerned Functional Department of the Company shall:

a) Retain an appropriate level of control over the Outsourced activity and the right to intervene with appropriate measures to continue the Company's business operations in

such cases without incurring prohibitive expenses and without any break in the operations of the Company and its services to its Customers;

b) Establish a viable contingency plan to consider the availability of alternative Service Providers or the possibility of bringing the Outsourced activity back in-house in an emergency, including having an understanding of the costs, time and resources that would be involved;
c) Maintain a central record of all Material Outsourcing, including sub-service providers, readily accessible for review by the Board and Senior Management of the Company. The records must be updated promptly and half-yearly reviews must be placed before the Board;
d) Review, at least on an annual basis, the financial and operational condition of the Service Provider to assess its ability to continue to meet its Outsourcing obligations. Such due diligence reviews, which shall be based on all available information about the Service Provider, must highlight any deterioration or breach in performance standards, confidentiality, and security, and in business continuity preparedness;
e) Immediately notify RBI in the event of any breach of security and leakage of confidential customer related information;
f) Ensure only need based access of Confidential Information is given to authorised staff/representatives of the Service Provider.
g) Review and monitor the security practices and control processes of the Service Provider on a regular basis and require the Service Provider to disclose security breaches;
h) Allow RBI or persons authorised by it to access the Outsourcing agreements, documents, records of transactions, and other information given to, stored or processed by the Service Provider;
i) Periodically review its Outsourcing arrangements to ensure that its Outsourcing risk management policies, procedures & guidelines are effectively complied with;
j) Periodically commission independent audit and expert assessments on the security and controls environment of the Service Provider. Such assessments and reports on the Service Provider must be performed and prepared by the Company's internal or external auditors, or by agents appointed by the Company.

8. Outsourcing Agreement

The terms and conditions governing the contract between the Company and the Service Provider shall be carefully defined in written agreements and vetted by the Company's legal counsel on their legal effect and enforceability, in accordance with the RBI Directions. Every such agreement shall address the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages.
The RBI directions mandate that the agreements with the Service Providers shall set forth the following provisions:

8.1 Clearly define what activities are going to be Outsourced including appropriate service and performance standards;
8.2 Ensure that the Company has the ability to access all books, records, and information relevant to the Outsourced activity available with the Service Provider;

8.3 Ensure continuous monitoring and assessment by the Company of the Service Provider so that any necessary corrective measures can be taken immediately;

8.4 A termination clause and minimum period to execute a termination provision, if deemed necessary;

8.5 Information about controls to ensure customer data confidentiality and the Service Provider's liability in case of breach of security and leakage of confidential customer related information;

8.6 Contingency plans to ensure business continuity;

8.7 Prior approval/ consent by the Company of the use of subcontractors by the Service Provider for all or part of an Outsourced activity;

8.8 The right to conduct audits on the Service Provider whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the Service Provider in conjunction with the services performed for the Company;

8.9 Clause to allow RBI or persons authorized by it to access the Company's documents, records of transactions, and other necessary information given to, stored or processed by the Service Provider within a reasonable time;

8.10 Clause to recognise the right of RBI to ask for an inspection to be made of the Company's Service Provider and its books and accounts by one or more of its officers, employees, or other person.

8.11 Ensure that confidentiality of the Customer's information shall be maintained even after the contract expires or is terminated;

8.12 Ensure that the Service Provider preserves documents as required by law and takes suitable steps to ensure that its interests are protected in this regard even post termination of the services;

8.13 Ensure that access to Customer Confidential Information by staff of the Service Provider shall be on a 'need to know' basis i.e., limited to those areas where the information is required in order to perform the Outsourced activity.

8.14 Ensure that the Service Provider is able to isolate and clearly identify the Company's customer information, documents, records and assets to protect the confidentiality of the information. In instances, where the Service Provider acts as an Outsourcing agent for multiple NBFCs, care shall be taken to build strong safeguards so that there is no comingling of information, documents, records, and assets.

8.15 Company's Service Providers to develop and establish a robust framework for documenting, maintaining, and testing business continuity and recovery procedures. The Company needs to ensure that the Service Provider periodically tests the business continuity and recovery plan and may also consider occasional joint testing and recovery exercises with its Service Provider.

9. Outsourcing within the Group/Conglomerate

a) The risk management practices to be adopted by the Company while Outsourcing to a related party (i.e., within the group/conglomerate, including holding or subsidiary or associate or a group company, whether located within or outside India) would be identical to those specified hereinabove along with those specified in the RBI Directions.

b) Due diligence on an intra-group Service Provider may take the form of evaluating qualitative aspects on the ability of the Service Provider to address risks specific to the Company, particularly those relating to business continuity management, monitoring and control, and audit and inspection, including confirmation on the right of access to be provided to RBI to retain effective supervision over the Company, and compliance with local regulatory standards.

c) The respective roles and responsibilities of each party in the Outsourcing arrangement must be documented in writing in a formal service level agreement with details like scope of services, charges for the services and maintaining confidentiality of the customer's data. It shall also incorporate a clause that there is a clear obligation for any Service Provider to comply with directions given by the RBI in relation to the Business Functions of the Company.

d) Such Outsourcing arrangements should not lead to any confusion to the Customers on whose products/services they are availing by clear physical demarcation of space where the activities of the Company and those of its other group entities are undertaken. Company must be able to identify & manage risk on a stand-alone basis.

e) RBI shall not be prevented from being able to obtain information required for the supervision of the Company or pertaining to the group as a whole.

10. Grievance Redressal

a) The Company shall have a Board approved Grievance Redressal Machinery which shall be placed on its website and the website of the Service Provider. An official shall be designated as the Grievance Redressal Officer for Outsourced activities. Similarly, an officer at each branch or office of the Company shall also be designated as 'Grievance Redressal Officer' for Outsourced activities.

b) The Company's Grievance Redressal Machinery will also deal with issues relating to services provided by the Service Provider.

11. Disclosure of outsourcing arrangements

The Company shall prominently publish on its website, the list of Service Providers engaged by them and Digital Lending Apps (DLAs) of the Company or the Service Provider with the details of the activities for which they have been engaged .

The Company shall communicate to the borrower, at the time of sanctioning of the loan and also at the time of passing on the recovery responsibilities to a Service Provider or change in the Service Provider responsible for recovery, the details of the Service Provider acting as recovery agent who is authorised to approach the borrower for recovery.

The Company shall ensure that the Service Provider, including Lending Service Provider, shall disclose upfront to the Customer, the name of the Company on its website / DLA / platform.

12. Reporting to FIU or other competent authorities

The Company shall submit Currency Transactions Reports (CTRs) and Suspicious Transactions Reports (STRs) to FIU or any other competent authority in respect to the Customer-related activities carried out by the Service Providers.

13. Responsibilities of DSA/ DMA/ DRA

The concerned Functional Head shall ensure that the DSAs/DMAs/DRAs are properly trained to handle their responsibilities with care and sensitivity, particularly aspects such as soliciting Customers, hours of calling, privacy of Customer information and conveying the correct terms and conditions of the products on offer, etc.

The Company obtain the undertaking of DSA/DMA/ recovery agents to abide by the Code of Conduct for DSAs/DMAs/DRAs, as provided in the Annexure). In addition, DRAs shall adhere to extant instructions on

the Fair Practices Code of the Company for collection of dues and repossession of security, if applicable. It is essential that the DRAs refrain from actions that could damage the integrity and reputation of the Company and that they observe strict Customer confidentiality.

The Company and its agents shall not resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts, including acts intended to humiliate publicly or intrude on the privacy of the debtor's family members, referees and friends, nor shall they make threatening and anonymous calls, or make false and misleading representations.

14. Offshore Outsourcing

a) The engagement of Service Providers in a foreign country exposes the Company to country risk, that is, economic, social and political conditions and events in a foreign country that may adversely affect the Company. Such conditions and events could prevent the Service Provider from carrying out the terms of its agreement with the Company. To manage the country risk involved in such Outsourcing activities, the Board and Senior Management shall take into account and closely monitor government policies, political, social, economic and legal conditions in countries where the Service Provider is based, during the risk assessment process and on a continuous basis, and establish sound procedures for dealing with country risk.

b) The Functional Department of the Company shall proactively evaluate such risks as part of the due diligence process and develop appropriate mitigating controls, contingency plans, and exit strategies. In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified. The Functional Head shall ensure the following:

   i) The activities Outsourced outside India shall be conducted in a manner so as not to obstruct or hinder efforts of the Company or regulatory authorities to perform periodic audits/inspections and assessments, supervise, or reconstruct the India activities of the Company based on books, records and necessary documentation, in a timely manner.

   ii) The Functional Department shall principally enter into arrangements with parties operating in jurisdictions that generally uphold confidentiality clauses and agreements.

   iii) The activities shall not be Outsourced within jurisdictions where access to books, records and any other information required for audit and review purposes may be impeded due to regulatory or administrative constraints.

   iv) The Outsourcing Team or Functional Heads shall notify the RBI when the rights of access for the Company and / or RBI are likely to be impeded.

   v) Emerging technologies such as data center hosting, applications as a service, and cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. The Functional Department should clarify the jurisdiction for their data and applicable regulations at the outset of an Outsourcing arrangement. This information should be reviewed periodically.

15. Business Continuity Planning

The concerned Functional Department should ensure that their business continuity preparedness is not adversely compromised on account of Outsourcing. The Functional Department should adopt sound business continuity management practices as issued by RBI and as per the Business Continuity planning and policies of the Company, and seek proactive assurance that the outsourced Service Provider maintains

readiness and preparedness for business continuity on an ongoing basis. The Functional Department, while framing the viable contingency plan, should consider the availability of alternative Service Providers or the possibility of bringing the Outsourced activity back-in house in case of an emergency (for example, where the number of vendors for a particular service is extremely limited), including understanding the costs, time and resources that would be involved, and take suitable preparatory action.

16. Review of the Policy

The Policy will be reviewed at yearly intervals or as and when considered necessary by the Senior Management/Board of the Company.

17. Change Control Record

Version No.	Change Request by	Memorandum of Change	Approval date
1.0	-	Adoption of policy by the Board of Directors of the Company	21.06.2023

Annexure: Code of Conduct for DSAs/ DMAs/ DRAs

Conduct by DSAs/DMAs

Tele-calling Process

a) A prospective customer may be contacted for prospect identification or sales only under the following circumstances:
   i) When the prospective customer expresses the desire to acquire a Financial Product through the website, tele-call centre, email service, SMS service, promotional event, or exhibition of the sales and promotion agents / subagents of the DSAs/DMAs.
   ii) When the prospective customer has been referred by another Customer or is an existing Customer of the Company who has given consent to accept calls for other products of the Company.
   iii) When the prospective customer has been referred by his/her employer under an arrangement with the Company.
   iv) When the prospective customer's name /telephone no. /address is available and obtained after taking his/her consent.

   Importantly, the employees/representatives of the DSA should not call a person whose name/number is flagged in any "Do Not Call" list made available to him/her.

b) Telephonic contact must normally be limited to the Prescribed Time only. However, it may be ensured that a prospective customer is contacted only when the call is not expected to inconvenience him/her.

c) Calls earlier or later than the Prescribed Time may be placed only when the prospective customer has expressly authorized the DSA/DMA and its employees/ representatives/ fieldsmen to do so either orally or in writing.

d) If the prospective customer is not available to attend the call, a message may be left for him/her. The aim of the message should be to get the prospective customer to return the call or to check for a convenient time to call again. Ordinarily, such messages may be restricted to:

> *"Hello, this is [name of officer] representing IBL Finance calling. I am requesting a call back at [phone number]."*

The message must indicate that the purpose of the call is with regard to selling, distributing, or marketing a product of the Company. The call must directly be made with the objective of emphasizing the endorsement of the Financial Product. The DSAs and their associated fieldsmen should strive to render their best services and guidance in communicating with the Customers.

e) Standard tele-calling etiquette (as specified below) should be practiced. The caller should identify himself, state the purpose of calling, educate the Customer about important terms and conditions of the Financial Product, and strive to endorse the brand on the advantages that the particular transaction can offer, as well as maintain a courteous disposition towards the Customer.

Tele-calling Etiquette

Pre Call

- No calls prior to or beyond the Prescribed Time unless specifically requested
- No serial dialing;
- No calling on lists unless list is cleared by the DSA/DMA team leader.

During Call

- Identify yourself, your company and your principal;
- Request permission to proceed;
- If denied permission, apologize and politely disconnect;
- State the reason for your call;
- Never interrupt or argue;
- To the extent possible, talk in the language which is most comfortable for the prospective customer;
- Keep the conversation limited to business matters, such that there is a professional touch to the dealings and conversations;
- Check for an understanding of the important terms and conditions by the Customer if he/she plans to buy the Financial Product;
- Reconfirm next call details;
- Provide your telephone number, your supervisor's name, or the Company's officer's contact details if asked by the Customer;
- Thank the Customer for his/her time and end the conversation politely and on a positive note.

Post Call

- Do not call Customers who have expressed their lack of interest in the offering for the next 3 months with the same offer;
- Provide feedback to the Company on Customers who have expressed their desire to be flagged "Do Not Call/ Do not Disturb";

- Never call or entertain calls from Customers regarding Financial Products already sold. Instead, advise them to contact the authorized representative of the Company.

No Misleading Statements / Misrepresentations Permitted

DSAs/DMAs and their employees/representatives should not:

i) Mislead the prospective customer on any Financial Product offered by the Company;
ii) Mislead the prospective customer about their business or the organization's name, or falsely represent themselves;
iii) Make any false/unauthorised commitment on behalf of the Company for any Financial Product.

Conduct by a DRA

Visiting / Calling Process

The DRAs and their employees/representatives, entrusted for the job of collections of payments due to the Company from its delinquent or defaulted Customers, shall:

i) not visit or call Customers other than at the Prescribed Time, unless the special circumstances of the Customer's business or occupation requires the DRA and its employees/representatives to contact them at a different time;
ii) maintain a log of all calls made to the delinquent/defaulted Customers along with a brief note on the outcome of the call;
iii) not make a demand for payment of an account by telephone, personal call or in writing, without indicating the name of the Company to whom the debt is owed, the balance of the account, and the identity and the basis of the claim of the person making the demand;
iv) not communicate with an employer, acquaintance, friend, relative or neighbour of the Customer for matters dealing to such recovery other than the reference contacts disclosed and consented by the Customer in the loan application;
v) respect the Customer's privacy;
vi) not disclose or threaten to disclose information about a debt which, with valid reason, is disputed by the Customer, without disclosing the fact that the Customer disputes such debt;
vii) not give to any person, by implication, inference or express statement, any false or misleading information that may be detrimental to the Customer, his or her spouse, or any member of his or her family.

Precautions to be Taken on Communications

The DRAs and their employees/representatives shall:

i) respect personal space and maintain adequate distance from the Customer;
ii) not enter the Customer's residence/office without his/her consent;
iii) not use muscle power for recovery of loans;
iv) not disclose or threaten to disclose information which could adversely affect the Customer's reputation for creditworthiness, when they know or have reason to suspect that the information is false;

v) not initiate or threaten to initiate communication with the Customer's employer prior to obtaining final judgment against the Customer, in order to exert pressure on the Customer. This does not prohibit the DRA and its employees/representatives from communicating with the Customer's employer solely to verify employment status or earnings or where an employer has an established debt counselling service or procedure;

vi) not give, or threaten to give, by implication, inference or statement, to the person who employs a Customer, his or her spouse or any member of his or her family, information that may adversely affect the employment or employment opportunities of the Customer, his or her spouse, or any member of his or her family;

vii) not use obscene, defamatory, abusive, or threatening language while communicating with the Customer or persons related to him/her or resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts;

For the purpose of this Code, intimidation and harassment shall include acts intended to humiliate publicly or intrude on the privacy of the Customer's family members, referees, and friends or make threatening and anonymous calls or make false and misleading representations.

Payments

i) The DRAs and their employees/representatives shall forward to the Company all payments within 24 hours of receipt from the Customers. No amount shall be retained/deducted by them as a collections fee.

ii) All payments received by the DRAs and their employees/representatives in respect of accounts assigned to them, collected in the form of cash/account payee cheque/bank draft/pay order payable to the Company, shall be deemed to have been collected only on realization of the amount by the Company.

iii) Any liability arising out of loss of cash or any other payment instrument shall be solely of the DRA and its employees/representatives and they shall be liable to make good to the Company the amount within 24 hours of such loss.

Issue of Receipts and Maintenance of Receipt Books

The DRAs and their employees/representatives are required to issue official receipts for all payments received using receipt books approved by the Company. All receipt books are to be used solely for the accounts assigned by the Company to the DRA. A register of such receipt books must be maintained by the DRAs and shall be available for inspection by the authorized representative of the Company upon request of the same.

Professional Representations and Conduct

The DRAs and their employees/representatives shall use their best efforts to ensure maximum recovery on all accounts. In the process of such debt recovery, the DRAs and their employees/representatives shall, at all times:

i) comply with all laws and regulations governing the conduct of debt collectors, commercial agents, and similar persons;
ii) not use any methods or tactics that are inconsistent with the policies of the Company nor should it harm the reputation of the Company. Should the DRAs and their employees/representatives have any doubt as to whether any method or tactic might contravene this, they shall consult the Company before employing such method or tactic and shall abide by any decision of the Company with respect thereto;
iii) not seek to secure the arrest or committal of any Customer;
iv) not do anything that can give a right to any person for a civil liability for tort or criminal liability.

General

Appearance and Dress Code

i) Employees/representatives of the Service Provider must be appropriately dressed and in proper attire while meeting with Customers:
   - For men, this means well-ironed trousers, and a well-ironed shirt, with the shirt sleeves preferably buttoned down.
   - For women, this means well-ironed formal attire (saree, suit, etc).
   - Jeans, t- shirts, and open sandals are not considered appropriate.
ii) The employees/representatives of the Service Provider should carry the identity card provided to them by the Service Provider. The identity card issued by the Service Provider should state the full name, designation of the employee/representative along with his/her photograph and the details of the Service Provider such as name, address and contact number. The employee/ representative must prominently display the identity card on their person.

Training and Conduct

i) The Service Provider must ensure that its employees/representatives and executives are properly trained to handle their responsibilities with sensitivity and care.
ii) No alcoholic beverages are to be consumed by the employees/representatives of the Service Provider while on the job.
iii) The Service Provider shall not during the execution of its duty, contract or sub-contract its duties and obligations, unless the same has been specifically permitted by the Company. Further, such contractors/sub-contractors shall abide by this Code while conducting such duties.

Gifts or Bribes

The employees/representatives of the Service Provider must not accept gifts or bribes of any kind from Customers. Any employee/representative of the Service Provider who is offered a bribe or payment of any kind by a Customer must report the offer to his/her management.

Handling of Letters and Other Communication

Any communication sent to the Customer should be in the mode and format approved by the Company.

Liability and Compensation

The Service Provider shall compensate the Company for any loss and/or damage caused to the Company as a consequence of any misconduct, illegal and/or criminal act or negligence on its part. In the event of

such a claim, the Company shall be entitled to realize the same from future or outstanding payments due to the Service Provider.

Use and Disclosure of Confidential Information

i) The Service Provider shall at all times respect the confidentiality and privacy of any information supplied by a Customer and shall be factual, truthful and tactful in using such information.
ii) The Service Provider shall respect the Customer's privacy. His/her interest may be discussed only with him/her and should only be discussed with any other individual/family member such as the Customer's accountant/ secretary/ spouse when authorised to do so by the Customer.
iii) The Service Provider must not use or disclose Confidential Information for any purpose other than the purpose for which the Confidential Information was provided to the Service Provider as set forth in the appointment letter along with its annexures.
iv) The Service Provider must agree to implement appropriate measures designed to ensure the security and confidentiality of Confidential Information, to protect such information against any anticipated threats or hazards to the security or integrity of such information, and to protect against unauthorized access to, or use of, Confidential Information that could result in substantial harm or inconvenience to any Customer of the Company or any of its subsidiaries, affiliates, or licensees.
v) On the termination of the service arrangement or agreement, the Service Provider shall hand over or cause to be handed over all such Confidential Information and all other related materials in the Service Provider's possession to the authorised representative of the Company.
vi) In the event of a breach or threatened breach by the Service Provider of this clause, monetary damages may not be an adequate remedy; therefore, the Company shall be entitled to injunctive relief to restrain the Service Provider from any such breach, threatened or actual.
vii) The Service Provider shall never allow any personal emotion or any unfriendly feelings towards any Customer to become evident in any dealings with such a Customer, but shall at all times retain a professional approach, and shall be guided in all dealings by sound principles and procedures of debt collection and debt management.

Reporting and Compliances

The Service Provider shall assist the Company to review its financial and operational conditions to assess their ability to continue to meet their outsourcing obligations. Such due diligence reviews, which can be based on all available information about the Service Provider shall highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

Events of Violation of the Code

The following will construe as events of violation of the Code by the Service Provider:

- The Company receives a written complaint from an aggrieved person or Customer with or without sufficient proof of violation of the Code, within 30 calendar days of the violation.
- There is a report of violation of the Code during any internal or regulatory audit of the Company's marketing, sales, or debt recovery process.

Punitive Action on Violation of the Code

In the event of violation of the Code, the Company will seek a written explanation from the concerned Service Provider and may, on its sole assessment, based on the seriousness and the extent of violation, take any one or more of the following actions:

a) Issue a written warning against the violation of the Code and seek details of control processes to be adopted by the Service Provider to avoid the recurrence of the violation;
b) Seek a detailed explanation of the Customer complaint;
c) Blacklist the erring employees of the Service Provider;
d) Permanently terminate the Service Provider with or without an advertisement in the newspaper informing the public that the said Service Provider has seized to be a representative of the Company;
e) Seek from the violating Service Provider reimbursement of any expenses incurred by the Company and/or payment of penalties levied by any competent authority on the Company due to violation of the Code.

Limitation

The Company would be responsible for the actions of its Service Provider and all other associated fieldsmen and the confidentiality of information pertaining to the Customer that is available with the Service Provider. Further, the Company shall retain ultimate control of the outsourced activity. The Company shall evaluate and guard against the various risks including the strategic risk, reputation risk, compliance risk, and operational risk that the Company may be subjected to from time to time.

****