Outsourcing Policy

I. Introduction:

'Outsourcing' is defined as the NBFC's use of a Third-Party hereafter referred as ("Service Provider") to perform activities on continuing basis that would normally be undertaken by the NBFC itself, now or in the future. 'Continuing basis' includes agreements for a limited period.
Typically, 'Outsourced financial services' includes applications processing (loan origination), document processing, marketing and research, supervision of loans, data processing and back office related activities, besides others.

II. Objectives & Regulatory Framework

RBI Directions

RBI has issued directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs. The directions are applicable to material outsourcing arrangements which may be entered into by an NBFC with a service provider located in India or elsewhere. The service provider may either be a member of the group/ conglomerate to which the NBFC belongs or an unrelated party.
These directions are concerned with managing risks in outsourcing of financial services and are not applicable to technology-related issues and activities which are not related to financial services, such as usage of courier, catering of staff, housekeeping and janitorial services, security of the premises, movement and archiving of records etc.

Activities that shall not be outsourced:
The Company if choose to outsource financial services shall not outsource the following services:

- Core management functions including internal audit, strategic and compliance functions
- Decision-making functions such as determining compliance with KYC norms
- Sanction of loans
- Management of investment portfolio

However, for NBFCs in a group/ conglomerate, these functions may be outsourced within the group subject to compliance with instructions elaborated below in outsourcing within the group.

Material Outsourcing Means
For the purpose of these directions, material outsourcing arrangements are those which, if disrupted, have the potential to significantly impact the business operations, reputation, profitability or customer service. Materiality of outsourcing would be based on various factors mentioned below:

- The level of importance to the NBFC of the activity being outsourced as well as the significance of the risk posed by outsourced activity;
- The potential impact of the outsourcing activity on the NBFC on various parameters such as earnings, solvency, liquidity, funding capital and risk profile;
- The likely impact on the NBFC's reputation and brand value, and ability to achieve its business objectives, strategy and plans, if the service provider fails to perform the services;
- The cost of the outsourcing activity as a proportion of total operating costs of the NBFC;

- The aggregate exposure to that particular service provider, in cases where the NBFC outsources various functions to the same service provider and
- The significance of activities outsourced in context of customer service and protection.

III. Roles & Responsibility

i.Roles & Responsibility of Board of Directors

- Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing activities and the policies that apply to such arrangements;
- Deciding on business activities of a material nature to be outsourced and approving such arrangements;
- Setting up suitable administrative framework of senior management for the purpose of these directions;
- Undertaking regular review of outsourcing strategies and arrangements for their continued relevance, safety and soundness;
- Shall take the responsibility for the actions of their service provider
- Shall take the responsibility to maintain the confidentiality of information pertaining to the customers that is available with the service provider;
- Shall ensure that the service provider, if not a group company of the Company, shall not be owned or controlled by any director of the Company or their relatives. These terms have the same meaning as assigned under Companies Act, 2013.

ii.Roles & Responsibility of Senior Management & Team

- Evaluating the risks and materiality of all existing and prospective outsourcing based on the framework approved by the Board;
- Developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing activity;
- Reviewing periodically the effectiveness of policies and procedures;
- Communicating information pertaining to material outsourcing risks to the Board in a timely manner;
- Ensuring that contingency plans, based on realistic and probable disruptive scenarios of service provider, are in place and tested;
- Ensuring that there is independent review and audit for compliance with set policies;
- Undertaking periodic review of outsourcing arrangements to identify new material outsourcing risks as they arise and

- Shall ensure to have a robust grievance redress mechanism, which in no way shall be compromised on account of outsourcing.

IV. Risk in Outsourcing

The key risks in outsourcing are Strategic Risk, Compliance Risk, Operational Risk, Legal Risk, Exit Strategy Risk, Counterparty Risk, Country Risk, Contractual Risk, Concentration and Systemic Risk. The failure of a service provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements by the service provider can lead to financial losses or loss of reputation for the Company.

The Company shall evaluate and guard against the following risks in outsourcing:

- Strategic Risk – Where the service provider conducts business on its own behalf, inconsistent with the overall strategic goals of the Company.
- Compliance Risk – Where privacy, consumer and prudential laws are not adequately complied with by the service provider.
- Operational Risk- Arising out of technology failure, fraud, error, inadequate financial capacity to fulfil obligations and/ or to provide remedies.
- Legal Risk – Where the Company may be subjected to fines, penalties, or punitive damages resulting from supervisory actions.
- Exit Strategy Risk – Where the Company may over-reliant on one firm, the loss of relevant skills in the Company itself preventing it from bringing the activity back in-house and contracts that make speedy exits prohibitively expensive.
- Counter party Risk – Where there is inappropriate underwriting or credit assessments.
- Contractual Risk – Where the Company may not have the ability to enforce the contract.
- 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.

V. Evaluation & Selection of Service Provider

In considering or renewing an outsourcing arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement. Due diligence shall take into consideration qualitative and quantitative, financial and operational factors.

The company shall conduct due diligence which shall involve an evaluation of all available information about the service provider, including but not limited to the following:

- Past experience and competence to implement and support the proposed activity over the contracted period;
- Financial soundness and ability to service commitments even under adverse conditions;
- Business reputation and culture, compliance, complaints and pending / potential litigations;

- Security and internal control, audit coverage, reporting and monitoring environment, business continuity management and ensuring due diligence by service provider of its employees.

Further if due diligence seems all right then the selection will be done as per the following criteria:

- Service Provider's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;
- Compatibility of the practices and systems of the service provider with the Company's requirements and objectives;
- Market feedback of the prospective service provider's business reputation and track record of their services rendered in the past;
- Level of concentration of the outsourced arrangements with a single party;

VI. Outsourcing Contract

The service provider may either be a member of the group/ conglomerate to which the NBFC belongs, or an unrelated party (collectively to be referred to as "Service Provider"),

1. Third Parties
2. Group Companies

The Company shall ensure the terms and conditions governing the contract with the service provider are carefully defined in written agreements and vetted by the Company's legal team on their legal effect and enforceability. Every such agreement shall address the risks and risk mitigation strategies. The agreement shall be sufficiently flexible to allow the Company to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement shall also bring out the nature of legal relationship between the parties.

The service provider agrees to the below:

- Ensure that appropriate service and performance standards and code of conduct (example no harassment where the outsourced service is collections) are adhered to as defined in the Agreement
- Have adequate financial capacity to fulfil obligations and/ or to provide remedies to the Company in the event of technology failure, fraud, error on part of Service Provider;
- Ensure that the Company has the ability to access all books, records and information relevant to the outsourced activity available with the service provider;
- The Company can continuous monitor and assess the service provider so that any necessary corrective measure can be taken immediately;
- Both parties have the right to terminate the Agreement as defined in the Termination clause of the agreement. In case of any material breach of any of the terms & conditions of the agreement, the agreement shall be terminated with immediate effect at the option of the non-defaulting party.

- It shall implement all necessary controls to ensure customer data confidentiality and it shall be service provider's liability in case of breach of security and leakage of confidential customer related information;
- The Service Provider shall review and monitor on regular basis and immediately disclose any breaches of security practice/processes and controls and leakage of Information to the Company. The Company shall also be entitled to review and monitor the security practices and control processes of the Service Provider on regular basis after providing reasonable prior notice.
- The service provider shall take prior approval/ consent of the Company for the use of subcontractors for all or part of an outsourced activity;
- It shall provide the Company with 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;
- The Company's documents, records of transactions, and other necessary information given to, stored or processed by the service provider shall be subject to on-site/off- site monitoring and inspection/scrutiny by the Reserve Bank of India or persons authorized by it. The service provider agrees to provide its books & accounts, records and information within 7 days upon receipt of notice from RBI;
- The confidentiality of customer's information shall be maintained even after the contract expires or gets terminated. The service provider shall preserve documents related to the Company and the customer as required by law and shall refrain from disclosing any information to unrelated third parties either implicitly or explicitly.
- The Company's Grievance Redressal Machinery will also deal with the issue relating to services provided by the service provider. Hence, the service provider shall respond to the grievances within the time frame fixed by the Company.

VII. Confidentiality and Security

Public confidence and customer trust are prerequisites for the stability and reputation of the Company. Hence the Company shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.

In this regard, the service provider shall ensure that:

- Access to customer information by staff of the service provider shall be on 'need to know' basis i.e. limited to those areas where the information is required in order to perform the outsourced function.
- 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.
- The Company shall be entitled to regular review and monitoring of the security practices and control processes of the service provider and the service provider shall disclose security breaches to the Company.

- The service provider shall immediately notify to the Company and RBI in the event of any breach of security and leakage of confidential customer related information.

VIII. Business Continuity and Management of Disaster Recovery Plan

The service provider agrees to the following:

- Develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. The service provider should periodically test the Business Continuity and Recovery Plan and allow the Company to test it too.
- The service providers should isolate the Company's information, documents and records, and other assets so that in appropriate situations, all documents, records of transactions and information given to the service provider, and assets of the Company, can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

IX. Monitoring and Control of Outsourced Activities

The service provider agrees to the following:

- The Company shall be entitled to at least on annual basis, review 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 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.
- The Company, in the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers, shall publicize by displaying at a prominent place in all the offices, posting it on the website, and informing the customers of the same so as to ensure that the customers do not continue to deal with the service provider.

INTRODUCTION

In accordance with Master Direction dated September 01, 2016 bearing reference number RBI/DNBR/2016-17/45 Master Direction DNBR.PD. PD.008/03.10/.119/2016-17 (as amended from to time) and RBI/2017-18/87 Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs DNBR.PD.CC. No.090/03.10.001/2017-18 November 09, 2017 (as amended from time to time) is required to put in place a comprehensive policy on outsourcing ("Outsourcing Guidelines"). In addition to the Outsourcing Guidelines, the Company is required to comply with and adhere to the Guidelines on Digital Lending dated September 2, 2022 issued and published by the Reserve Bank of India ("RBI") vide its circular being reference number RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 ("Digital Lending Guidelines") in respect of the outsourcing arrangements entered by the Company with a Lending Service Provider ("LSP") / Digital Lending App ("DLA"). "Outsourcing" is defined as the a non-banking financial company's (NBFC) use of a third-party (hereafter referred as "Service Provider") to perform activities on continuing basis that

would normally be undertaken by the NBFC itself, now or in the future. 'Continuing basis' includes agreements for a limited period. Typically, outsourced financial services includes applications processing (loan origination), document processing, marketing and research, supervision of loans, data processing and back office related activities, besides others.

OBJECTIVES & REGULATORY FRAMEWORK

The Company intending to outsource any of its financial activities shall put in place a comprehensive outsourcing policy approved by its Board, which incorporates, inter alia criteria for selection of such activities as well as Service Providers, delegation of authority depending on risks and materiality and systems to monitor and review the operations of these activities. The objective of having policy in place for outsourcing activity is to protect the interest of the customers and the investors of the Company and to ensure that the Company and the RBI have access to all relevant books, records and information available with Service Provider and to ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and RBI nor impede effective supervision by RBI. The Company therefore shall take steps to ensure that the Service Provider employs the same high standard of care in performing the services as is expected to be employed by the Company, as if the activities were conducted within the Company and not outsourced. Accordingly, the Company shall not engage in outsourcing that would result in the Company's internal control, business conduct or reputation being compromised or weakened.

RBI Directions

RBI has issued directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs. The directions are applicable to material outsourcing arrangements which may be entered into by an NBFC with a Service Provider located in India or elsewhere. The Service Provider may either be a member of the group/ conglomerate to which the NBFC belongs or an unrelated party. These directions are concerned with managing risks in outsourcing of financial services and are not applicable to technology-related issues and activities which are not related to financial services, such as usage of courier, catering of staff, housekeeping and janitorial services, security of the premises, movement and archiving of records etc.

The RBI has, vide the Digital Lending Guidelines, has mandate that outsourcing arrangements entered by regulated entities (as defined in the Digital Lending Guidelines) with a LSPs and DLAs does not diminish the relevant regulated entity's obligations and they shall continue to conform to the Digital Lending Guidelines. The REs are advised to ensure that the LSPs engaged by them and the DLAs (either of the RE or of the LSP engaged by the RE) comply with the guidelines contained in this circular

Activities that shall not be outsourced

The Company if chooses to outsource financial services shall not outsource following services:

(a) Core management functions including internal audit, strategic and compliance functions;

(b) Decision-making functions such as determining compliance with KYC norms;

(c) Sanction of loans;

(d) Management of investment portfolio.

However, for NBFCs in a group/ conglomerate, these functions may be outsourced within the group subject to compliance with instructions elaborated below in outsourcing within the group.

Material Outsourcing

For the purpose of this Policy, means material outsourcing arrangements are those which, if disrupted, have the potential to significantly impact the business operations, reputation, profitability or customer service. Materiality of outsourcing would be based on various factors mentioned below:
(a) The level of importance to the NBFC of the activity being outsourced as well as the significance of the risk posed by outsourced activity;
(b) The potential impact of the outsourcing activity on the NBFC on various parameters such as earnings, solvency, liquidity, funding capital and risk profile;
(c) The likely impact on the NBFC's reputation and brand value, and ability to achieve its business objectives, strategy and plans, if the Service Provider fails to perform the services;
(d) The cost of the outsourcing activity as a proportion of total operating costs of the NBFC;
(e) The aggregate exposure to that particular Service Provider, in cases where the NBFC outsources various functions to the same Service Provider; and
(f) The significance of activities outsourced in context of customer service and protection.

ROLES & RESPONSIBILITIES

Roles & Responsibility of Board of Directors

(a) Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing activities and the policies that apply to such arrangements;
(b) Deciding on business activities of a material nature to be outsourced and approving such arrangements;
(c) Setting up suitable administrative framework of senior management for the purpose of these directions;
(d) Undertaking regular review of outsourcing strategies and arrangements for their continued relevance, safety and soundness;
(e) Undertaking responsibility for the actions of their Service Provider;
(f) Undertaking responsibility to maintain the confidentiality of information pertaining to the customers that is available with the Service Provider;
(g) Undertake to ensure that the Service Provider, if not a group company of the Company, shall not be owned or controlled by any director of the Company or their relatives. These terms have the same meaning as assigned under Companies Act, 2013.

Roles & Responsibility of Senior Management & Team

(a) Evaluating the risks and materiality of all existing and prospective outsourcing based on the framework approved by the Board;
(b) Developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing activity;
(c) Reviewing periodically the effectiveness of policies and procedures;
(d) Communicating information pertaining to material outsourcing risks to the Board in a timely manner;
(e) Ensuring that contingency plans, based on realistic and probable disruptive scenarios of Service

Provider, are in place and tested;
(f) Ensuring that there is independent review and audit for compliance with set policies;
(g) Undertaking periodic review of outsourcing arrangements to identify new material outsourcing risks as they arise;
(h) Ensuring to have a robust grievance redress mechanism, which in no way shall be compromised on account of outsourcing.

RISKS IN OUTSOURCING

The key risks in outsourcing are Strategic Risk, Compliance Risk, Operational Risk, Legal Risk, Exit Strategy Risk, Counterparty Risk, Country Risk, Contractual Risk, Concentration and Systemic Risk. The failure of a Service Provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements by the Service Provider can lead to financial losses or loss of reputation for the Company. The Company shall evaluate and guard against the following risks in outsourcing:
(a) Strategic Risk – Where the Service Provider conducts business on its own behalf, inconsistent with the overall strategic goals of the Company;
(b) Compliance Risk – Where privacy, consumer and prudential laws are not adequately complied with by the Service Provider;
(c) Operational Risk – Arising out of technology failure, fraud, error, inadequate financial capacity to fulfil obligations and/ or to provide remedies;
(d) Legal Risk – Where the Company may be subjected to fines, penalties, or punitive damages resulting from supervisory actions;
(e) Exit Strategy Risk – Where the Company may over-reliant on one firm, the loss of relevant skills in the Company itself preventing it from bringing the activity back in-house and contracts that make speedy exits prohibitively expensive;
(f) Counter party Risk – Where there is inappropriate underwriting or credit assessments;
(g) Contractual Risk – Where the Company may not have the ability to enforce the contract;
(h) 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.

EVALUATION AND SELECTION OF SERVICE PROVIDER

In considering or renewing an outsourcing arrangement, appropriate due diligence shall be performed to assess the capability of the Service Provider to comply with obligations in the outsourcing agreement. Due diligence shall take into consideration qualitative and quantitative, financial and operational factors. The Company shall consider whether the Service Provider's systems are compatible with its own and also whether their standards of performance including in the area of customer service are acceptable to it. The Company shall also consider, issues relating to undue concentration of outsourcing arrangements with a single Service Provider. Where ever possible, the Company shall obtain independent reviews and market feedback on the Service Provider to supplement its own findings. Due diligence shall involve an evaluation of all available information about the Service Provider, including but not limited to the following:
(a) Past experience and competence to implement and support the proposed activity over the contracted period;

(b) Financial soundness and ability to service commitments even under adverse conditions;
(c) Business reputation and culture, compliance, complaints and pending / potential litigations;
(d) Security and internal control, audit coverage, reporting and monitoring environment, business continuity management and ensuring due diligence by Service Provider of its employees.
Further if due diligence seems all right then the selection should be done as follows:
(a) Service Provider's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;
(b) Compatibility of the practices and systems of the Service Provider with the Company's requirements and objectives;
(c) Market feedback of the prospective Service Provider's business reputation and track record of their services rendered in the past;
(d) Level of concentration of the outsourced arrangements with a single party.

OUTSOURCING CONTRACTS

The Company shall ensure the terms and conditions governing the contract with the Service Provider are carefully defined in written agreements and vetted by the Company's legal team on their legal effect and enforceability. Every such agreement shall address the risks and risk mitigation strategies. The agreement shall be sufficiently flexible to allow the Company to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement shall also bring out the nature of legal relationship between the parties.
The Company will consider some of the key provisions while entering into contract with the Service Provider, which are mentioned below:
(a) The contract shall clearly define what activities are going to be outsourced including appropriate service and performance standards;
(b) Ensure that the Company has the ability to access all books, records and information relevant to the outsourced activity available with the Service Provider;
(c) The contract shall provide for continuous monitoring and assessment by the Company of the Service Provider so that any necessary corrective measure can be taken immediately;
(d) Termination clause and minimum period to execute a termination provision, if deemed necessary shall be included;
(e) Controls to ensure customer data confidentiality and Service providers liability in case of breach of security and leakage of confidential customer related information shall being incorporated;
(f) The contract shall provide for the prior approval/ consent by the Company of the use of subcontractors by the Service Provider for all or part of an outsourced activity;
(g) It shall provide the Company with 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;
(h) Outsourcing agreements shall include clauses to allow the 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;
(i) Outsourcing agreement shall also include a clause to recognize the right of the RBI to cause an inspection to be made of a Service Provider of the Company and its books and account by one or more of its officers or employees or other persons;
(j) The outsourcing agreement shall also provide that confidentiality of customer's information shall be

maintained even after the contract expires or gets terminated and the Company shall have necessary provisions to ensure that the Service Provider preserves documents as required by law and take suitable steps to ensure that its interests are protected in this regard even post termination of the services.

Further care shall be taken to ensure that the outsourcing contract:

(a) Clearly defines what activities are going to be outsourced, including appropriate service and performance levels;
(b) Provides for mutual rights, obligations and responsibilities of the Company and the Service Provider, including indemnity by the parties;
(c) Provides for the liability of the Service Provider to the Company for unsatisfactory performance/other breach of the contract;
(d) Specifies the responsibilities of the Service Provider with respect to the information technology security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.

DIGITAL LENDING

Loan Disbursements

Digital lending has been defined as a remote and automated lending process, largely by use of seamless digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service. Digital lending is catered to borrowers through DLAs (including platforms being mobile and web-based applications with user interface that facilitate digital lending services). DLAs will include apps of the Company as well as those operated by LSPs (being agent of the Company who carries out one or more of lender's functions or part thereof in customer acquisition, underwriting support, pricing support, servicing, monitoring, recovery of specific loan or loan portfolio on behalf of the Company in conformity with extant Outsourcing Guidelines).
For loans disbursed through DLAs or sourced through LSPs, the Company ensures that all loan servicing, repayment, etc., is executed by the borrower directly in the Company's bank account without any pass-through account/ pool account of any third party. The Company does not disburse such loans to a third-party account, including the accounts of LSPs and their DLAs.

Disclosures

All commercials details in relation to the loans disbursed through the DLAs or LSPs are disclosed upfront to the borrowers vide a key fact statement (in the format set out in the Digital Lending Guidelines).
The Company discloses the following on its website, from time to time, in respect of the loan products disbursed through the DLAs / LSPs:
(a) List of LSPs;
(b) Brief of loan products disbursed through DLAs / LSPs;
(c) Details of recovery agent.

Due Diligence

The Company conducts due diligence on the LSP / DLA and undertakes periodic review of the LSP / DLAs. The Company has authorised it's personnel to impact necessary and timely guidance to LSPs acting as recovery agent to comply with the norms, guidelines and instructions prescribed by the RBI.

Nodal Grievance Redressal Officer

The Company has appointed a suitable nodal grievance redressal officer to deal with fintech/ digital lending related complaints/ issues raised by the borrowers. The name and details of such officer along with the process of grievance redressal is set out on the website of the Company.

CONFIDENTIALITY & SECURITY

Public confidence and customer trust are prerequisites for the stability and reputation of the Company. Hence the Company shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the Service Provider. The Company shall ensure that:
(a) Access to customer information by staff of the Service Provider shall be on 'need to know' basis i.e. limited to those areas where the information is required in order to perform the outsourced function;
(b) 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 Service Provider acts as an outsourcing agent for multiple NBFCs, care shall be taken to build strong safeguards so that there is no commingling of information / documents, records and assets;
(c) Regular review and monitoring of the security practices and control processes of the Service Provider and require the Service Provider to disclose security breaches; (d) Immediate notifying to RBI in the event of any breach of security and leakage of confidential customer related information;
(e) No information (including personal information or data of the borrowers) shall be collected by LSPs / DLAs without the prior explicit consent of the borrowers;
(f) All data collection by the Company is stored in the servers located in India.
Nothing stated above shall preclude the Company from adhere to the mandate of disclosing / reports borrowers to the credit information companies in accordance with the Digital Lending Guidelines and/or the Outsourcing Policies and/or other extant instructions / guidelines / directions / circulars of the RBI.

BUSINESS CONTINUITY AND MANAGEMENT OF DISASTER RECOVERY PLAN

The Company shall require its Service Providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. The Company shall 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.
In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the Service Provider, the Company shall retain an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the Company and its services to the customers. In establishing a viable contingency plan, the Company shall consider the availability of alternative Service Providers or the possibility of bringing the outsourced activity back in-house in an emergency and the costs, time and resources that would be involved. The Company will make sure that

Service Providers are able to isolate the Company's information, documents and records, and other assets so that in appropriate situations, all documents, records of transactions and information given to the Service Provider, and assets of the Company, can be removed from the possession of the Service Provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

MONITORING AND CONTROL OF OUTSOURCED ACTIVITIES

A central record of all material outsourcing that is readily accessible for review by the Board and senior management of the Company shall be maintained. The records shall be updated promptly and on half yearly basis reviews shall be placed before the Board or Risk Management Committee. Regular audits would be done by either the internal auditors or external auditors of the Company to assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement. The Company shall at least on an annual basis, review 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 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. In the event of termination of the outsourcing agreement for any reason in cases where the Service Provider deals with the customers, the same shall be publicized by displaying at a prominent place in all the offices, posting it on the website, and informing the customers so as to ensure that the customers do not continue to deal with the Service Provider.

OUTSOURCING WITHIN GROUP

In a group structure, the Company may have back-office and service arrangements/ agreements with group entities e.g. sharing of premises, legal and other professional services, and hardware and software applications, centralize back-office functions, outsourcing certain financial services to other group entities etc. Before entering into such arrangements with group entities the Company shall have an arrangement with their group entities which shall also cover demarcation of sharing resources i.e. premises, personnel, etc. Moreover, the customers shall be informed specifically about the company which is actually offering the product/ service, wherever there are multiple group entities involved or any cross selling observed. While entering into such arrangements, the Company shall ensure that:

(a) Arrangements are appropriately documented in written agreements with details like scope of services, charges for the services and maintaining confidentiality of the customer's data;

(b) Such arrangement does not lead to any confusion to the customers on whose products/ services they are availing by clear physical demarcation of the space where the activities of the Company and those of its other group entities are undertaken;

(c) Incorporate a clause under the written agreements that there is a clear obligation for any Service Provider to comply with directions given by the RBI in relation to the activities of the Company;

(d) The Company shall ensure that their ability to carry out their operations in a sound fashion would not be affected if premises or other services (such as information technology systems, support staff) provided by the group entities become unavailable;

(e) If the premises of the Company are shared with the group entities for the purpose of cross-selling, the Company shall take measures to ensure that the Company's identification is distinctly visible and clear to the customers. The marketing brochure used by the group entity and verbal communication by its staff / agent in the Company premises shall mention nature of arrangement of the entity with the Company so

that the customers are clear on the seller of the product;
(f) The Company shall not publish any advertisement or enter into any agreement stating or suggesting or giving tacit impression that they are in any way responsible for the obligations of its group entities.

REVIEW OF THIS POLICY

This policy document will be reviewed and revised by the business team with approval of board of directors in response to changed circumstances, and in any event, at intervals of not more than half year or shorter review periods as may be stipulated by the board of directors.

IMPLEMENTATION

This Policy shall be effective from the date of adoption by the Board.

AMENDMENT

This Policy shall be amended and/or restated and updated from time to time and such amendments and/or restatements and updations shall be effective from the date of adoption by the Board.

Pioneer Financial & Management Services Limited ("**Pioneer**"), an NBFC regulated by the Reserve Bank of India (RBI) may, subject to extant regulations, outsource its certain activities to the service provider/s. While undertaking the outsourcing activity from Pioneer, service provider shall be deemed to have read and accepted the below mentioned Outsourcing Terms & Conditions ("**T&Cs**"). The T&C's are framed in view of directions issued by the RBI and as such service provider shall follow the T&Cs to the extent relevant to their activity.

Outsourcing Terms and Conditions ("T&Cs"):

This Schedule shall form an integral part of the Outsourcing Agreement ("**Agreement**").

Definitions:

- *Outsourcing:*
  Outsourcing is defined as the NBFC'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 activities on a continuing basis ('Continuing basis' includes agreements for a limited period) that would normally be undertaken by the NBFC itself, now or in the future.

- *Material Outsourcing:*

Material outsourcing arrangements are those which, if disrupted, have the potential to significantly impact the business operations, reputation, profitability or customer service.

Outsourcing guidelines prescribes two sets of outsourcing partners for NBFC:

The service provider may either be a member of the group/ conglomerate to which the NBFC belongs, or an unrelated party (collectively to be referred to as "**Service Provider**"),

1. Third Parties
2. Group Companies

Terms & Conditions for Outsourcing activities:

Any activity outsourced by Pioneer to the Service Provider shall be subject to the following general terms and conditions:

- The Service Provider shall,
  - adhere to all the applicable laws, rules, regulations, conditions of approval related to licensing or registration, guidelines and/or directives, as may be amended from time to time, issued to and/or applicable to Pioneer as well as the Service Provider, by a statutory or regulatory authority as may be applicable from time to time, with respect to the Services and other subject matter hereof;
  - act with all reasonable diligence, in good faith, observe all instructions of Pioneer from time to time and shall follow fair practices to maintain privacy, consumer and prudential laws;
  - not carry out any activity that would result in internal control, business conduct or reputation of Pioneer being compromised or weakened;

- not conduct business on its own behalf, inconsistent with the overall strategic goals of Pioneer;
- have adequate financial capacity to fulfil obligations and/ or to provide remedies to Pioneer in the event of technology failure, fraud, error on part of the Service Provider;
- not assign, delegate or subcontract any of its responsibilities contained in the Agreement to any agent, sub-agent or sub-contractor without prior written consent/permission of Pioneer. The agreement in respect of services shall be on Principal-to-Principal basis.
- strictly adhere to internal guidelines, policies and standards as may be issued by Pioneer from time to time that are duly shared with the Service Provider;
- ensure reasonable standards of care and skill in discharging the Services in terms of the Agreement.
- put in place appropriate procedures and policies to restrict its employees, consultants or other agents from causing breach under the Agreement. It shall promptly notify Pioneer of any such breach;
- segregate and keep separately and hold in trust all information, documents and record and other assets pertaining to the Services and relating to Pioneer;
- take adequate measure to ensure that the Services by the Service Provider at the relevant places are distinctly visible and clear to customers, in the event the Service Provider is sharing the premises with other persons.

- In case the Service Provider is an offshore entity then (i) the services shall be confined to limited activities by which Pioneer is not subjected to or governed by any regulations or laws in such off shore jurisdiction. and (ii) also, the jurisdiction of the courts in the off shore location where data is maintained shall not extend to the operations of Pioneer in India on the strength of the fact that the data is being processed there even though the actual transactions are undertaken in India; and (iii) further all original records shall continue to be maintained in India by Pioneer and hence the service agreement /arrangement shall be governed accordingly.
- **Confidentiality & Security:**
    - The Service Provider recognises that in the course of the transactions envisaged by the Agreement, it may be privy to certain confidential information (regardless of whether such information is expressly marked or designated as "confidential" or "proprietary") relating to Pioneer and its businesses including legal, financial, technical, commercial, marketing and business related records, data, documents, reports, etc., client/customer information, the terms of the Agreement and the details of the negotiations between the Parties (the "**Information**"). The Service Provider agrees that:
        - it shall keep all Information and other materials passing from Pioneer to the Service Provider confidential and shall not, without the prior written consent of Pioneer, divulge such Information to any other person or use such Information other than for the purposes of carrying out the Agreement;
        - it shall take all steps as may be reasonably necessary to protect the integrity of the Information and to ensure against any unauthorized disclosure thereof;

- The Service Provider, it's employees, agents, and subcontractors shall treat all records and information containing Personal Information acquired or generated as a result of the Agreement in strict confidence and with the care and security required to ensure they are not disclosed or made known to any person except in accordance with the Agreement and shall promptly inform Pioneer of any potential or accidental disclosure of the Information and take all steps, together with Pioneer, to retrieve and protect the said Information;
- It shall inform Pioneer immediately upon it becoming aware of any unauthorized access, collection, use, disclosure or destruction of Records and information containing Personal Information relating to the Agreement;
- It shall ensure that the Personnel and all its employees and/or representatives who are given access to the Information shall at all times be bound by legally valid and written non-disclosure obligations under their employment contracts; and
- It shall limit access to all Information on need-to-know basis, to only those of Service Provider's personnel, agents and representatives who need to know such information for carrying out Pioneer obligations for the purposes of carrying out the Agreement.
- It shall use the Information only for the purpose for which it was provided and not profit from the same in an unauthorized manner to the exclusion of Pioneer.

- All the Confidentiality obligations applicable to the Service Provider under the Agreement, shall be made applicable to all the employees, affiliates, agents, representatives, advisers, consultants, or such other persons with whom such Information is shared by the Service Provider. Upon expiry or termination of the Agreement or upon receipt of a request from Pioneer, the Service Provider shall return to Pioneer all Information received by it or destroy all such Information and certify in writing to such destruction.
- The Service Provider shall ensure that, other than in the course of and for the purpose of rendering services to Pioneer, the Information will not be copied, reproduced, reengineered, reverse engineered or transmitted by any means and in any form whatsoever (including in an externally accessible computer or electronic information retrieval system) by the Service Provider or its representatives without the prior written permission of Pioneer.
- The Service Provider shall maintain the confidentiality of the Information by exercising no lesser security and control measures and degree of care than those which the Service Provider applies to its own confidential information.
- The Service Provider shall fully indemnify Pioneer for any loss, damage caused due to breach and/or leakage of confidential Information of Pioneer and/or violation of any applicable laws.
- Pioneer shall have the right to review and monitor the security practices and control processes of the Service Provider on a regular basis and may require the Service Provider to disclose any security breaches.

- The Service Provider shall ensure that they have adequate safeguards to ensure that there is no combining/co-mingling of information, documents, records and assets of Pioneer in case the Service Provider is acting as an outsourcing agent for multiple entities.
- The Service Provider shall also preserve all the documents under the Agreement as required under the applicable laws and shall take suitable steps to ensure that Pioneer's interests are protected in this regard even post termination of the Services.
- The obligations contained in this Section shall not apply to any part of the Information in the case where that part of the Information that is or has become public (other than by breach of the Agreement) and shall not restrict any disclosure by the Service Provider required by law or by any court of competent jurisdiction, any enquiry or investigation by any governmental, official or regulatory body which is lawfully entitled to require any such disclosure, provided that, so far as it is lawful and practical to do so prior to such disclosure, the Service Provider when subject to such disclosure shall promptly notify Pioneer of such requirement with a view to providing the opportunity for Pioneer to contest such disclosure or otherwise to agree the timing and content of such disclosure.
- The obligations contained in this Section shall continue to apply after the termination or expiry of the Agreement.
- The Service Provider shall, on written demand of Pioneer immediately return Information together with any copies in its possession.
- The Service Provider acknowledges that in the event of any breach or threatened breach of this Section by the Service Provider/its employees/agents/sub-contractors, monetary damages may not be an adequate remedy, and therefore, Pioneer shall be entitled to injunctive relief to restrain the Service Provider/its employees/agents/sub-contractors from any such breach, actual or threatened.
- The Service Provider shall carefully preserves all the documents containing customer related Information, data etc., as required by the law and shall refrain from disclosing any information to unrelated third parties either implicitly or explicitly, irrespective of any divergence in views and breakdown of professional relationships or any disputes or dissatisfaction between the parties, in any manner that would jeopardize the business and corporate reputation of the Pioneer. The Service Provider and its employees, agents, assigns shall not allow access or share such documentation in part or whole to any third party, or allow any third party to unless obliged to do so by any regulatory authority or a court of law having competent jurisdiction to mandate such sharing or access.
- The Service Provider shall act, follow and provide its Services in accordance with the Fair Practices Code and other directions as issued and amended by Reserve Bank of India from time to time and as displayed on Pioneer's website ("https://www.Pioneer.com"), failing which it shall be deemed to be a material breach of the terms of the Agreement.

- **Security and Control Processes:**
  - The Service Provider hereby agrees to have reasonable security practices, control processes and checks in respect of the sourcing, servicing and collections on a regular basis to the extent directed by Pioneer and as per the applicable laws including the provisions of Information Technology Act, 2000.

- The Service Provider shall review and monitor on a regular basis and immediately disclose any breaches of security practice/processes and controls and leakage of Information to Pioneer. Pioneer shall also be entitled to review and monitor the security practices and control processes of the Service Provider on a regular basis after providing reasonable a prior notice.

- **Data Privacy**
  - The Service Provider (and shall procure that the Service Provider's personnel) shall comply with all Data Protection Legislation and such compliance shall include, but not be limited to, maintaining a valid and up to date registration or notification (where applicable) under the Data Protection Legislation.
  - For this purpose,
- "**Data Protection Legislation**" means the legislation and regulations relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual including (without limitation):
  - the Information Technology Act, 2000 (as amended from time to time), including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules") and any other applicable rules framed thereunder;
  - all other industry guidelines (whether statutory or non-statutory) or codes of conduct relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual issued by any regulator to Pioneer; and
  - any other applicable law solely relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual.
- "**Personal Data**" shall have the same meaning as ascribed to the term 'Sensitive Personal Data or Information' under the Privacy Rules (as amended from time to time).

  - The Service Provider shall only undertake the processing of Personal Data:
- reasonably required in connection with the performance of its obligations under the Agreement; and
- in accordance with the Pioneer's written instructions, and,
- shall comply with all reasonable procedures and processes notified by Pioneer from time to time.
  - Pioneer hereby instructs the Service Provider to take such steps in the processing of Personal Data on behalf of Pioneer as are reasonably necessary for their performance of the Service Provider's obligations under the Agreement.
  - The Service Provider shall not process or transfer any Personal Data outside India without the prior written consent of Pioneer.

- The Service Provider shall at all times have appropriate technical and organisational measures in place acceptable to Pioneer:

- To prevent unauthorised or unlawful processing of any Personal Data;
- To protect any Personal Data against accidental loss, destruction or damage;
- To ensure the reliability of its personnel having access to the Personal Data;
- On Pioneer's reasonable request, the Service Provider will:
- provide a detailed, written description of the measures undertaken by the Service Provider and the Service Provider's compliance with those measures; and
- allow Pioneer access to the Service Provider's premises to inspect its procedures for the processing of Personal Data;
- If the Service Provider receives a request from any person for access to Personal Data or any other request relating to Pioneer's obligations under the Data Protection Legislation the Service Provider shall:-
- immediately notify Pioneer; and
- provide full co-operation and assistance to Pioneer in relation to any such complaint or request including, without limitation:
- provide Pioneer with full details of any such request;
- provide Pioneer with any Personal Data it holds in relation to any person in a form specified by the Pioneer and within [?] days of receipt of the request from any person or as otherwise stipulated by Pioneer; and
- comply with the data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with explicit authorisation to do so from Pioneer;
- The Service Provider shall:
- immediately provide Pioneer with full details of any complaint or allegation that it is not complying with the Data Protection Legislation; and
- assist Pioneer in taking any action that Pioneer deems appropriate to deal with such complaint or allegation including without limitation immediately providing Pioneer with any Personal Data it holds in relation to any person.
- **Audit and Inspection:**
    - The Service Provider shall keep complete records and details of financial transactions including invoices, payments received and tax remitted in connection with the Services provided to Pioneer. All the aforesaid records shall be kept on file by the Service Provider for a period of Ten (10) years from the date the record is made.
    - The Service Provider shall at all times, upon 07 (seven) business days written notice, allow Pioneer, its management and/or its auditors and/or its regulators (including external regulators and auditors) and /or its promoters, the opportunity of inspecting, examining

and auditing, the Service Provider's operations and business / financial / operational records / documents which are directly relevant to the Services contemplated hereunder, its balance sheet and profit and loss account and audit reports, for the purposes of ascertaining the financial viability of the Service Provider.

- As and when required by Pioneer, and upon prior notice of at least 02 (Two) business days the Service Provider shall provide access to and make available to any of Pioneer's authorized officers / employees/ management or internal / external auditors / promoters, the necessary records for inspection / examination / audit, and co-operate to the fullest extent so as to clarify on any activities and to assure a prompt and accurate audit related to the Scope of Services.
- The Service Provider shall co-operate with Pioneer's internal or external auditor or other person to assure a prompt and accurate audit (specific to the Services).
- The Service Provider shall also co-operate in good faith with Pioneer to correct any practices which are found to be deficient as a result of any such audit, within a reasonable time, as may be agreeable to Pioneer.
- The Service Provider agrees that RBI/any other competent authority or persons authorised by RBI shall be entitled to access the records of transactions, IT Infrastructure, applications, data, documents and other necessary information given to, stored or processed by the Service Provider in relation to the Services.
- RBI and Pioneer shall be entitled to cause an inspection to be made on the Service Provider and any of its sub-contractors and their IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the Service Provider and/ or its sub-contractors and their books, records, information and account by one or more of its Personnel including officers or employees or other persons.
- The Service Provider shall maintain its regular books of accounts, records and any other information in respect of the Services and relevant to the outsourced activity. The Service Provider shall provide to Pioneer, its management, its auditors (internal & external) and/or its regulators, agents appointed to act on behalf of Pioneer, or any other person authorized by it, unrestricted and effective access to the Service Provider's business premises, operations/business records, logs, alerts, data for the purposes of performing and conducting audits / inspection, spot checks and to obtain such copies of any audit or review reports and findings made on the Service Provider (including its sub-contractors).
- The Service Provider agrees and acknowledges that the Pioneer shall be entitled to conduct a periodic and/or continuous monitoring and assessment of the Service Provider (including the financial and operational conditions of the Service Provider) so as to take any necessary corrective measures immediately.

- **Business Continuity**
  - The Service Provider has and will maintain throughout the term of the Agreement a business continuity, disaster recovery, and backup capabilities and facilities ("**BCP**") to enable it to recover and resume the Services provided by it to Pioneer under the

Agreement within [1 (one) Business Day] from the occurrence of an event/ incident which disrupts or has a significant impact on the performance of the Services by the Service Provider ("**Interruption Event**"). The Service Provider hereby confirms that it has tested its BCP and will continue to conduct sufficient ongoing verification and testing for the BCP and recovery and resumption of services. The Service Provider will update its BCP at least annually. Pioneer at its discretion may cause the Service Provider to undertake joint testing and recovery exercises.

- The Service Provider will promptly notify Pioneer of any actual, threatened, or anticipated Interruption Event and will cooperate fully with Pioneer to minimize and remedy any such disruption and promptly restore and recover the Services. Further, the Service Provider acknowledges and agrees that upon the occurrence of an Interruption Event, Pioneer has a right to intervene with appropriate measures to continue business operations/ services, without causing any break in the operations of Pioneer and its Services. All cost and expenses incurred by Pioneer in connection with the aforesaid right of intervention shall be borne by the Service Provider.
- The Service Provider further acknowledges and agrees that (a) the Service Provider shall at all times isolate Pioneer's information, documents and records, and other assets; and (b) upon the occurrence of default by the Service Provider of its obligation under the Agreement or the occurrence of an Interruption Event, Pioneer has a right in its sole discretion (and without prejudice to its other rights under the Agreement), to cause the removal (by deletion, destroying or rendering unusable or otherwise) from the possession of the Service Provider, all documents, records of transactions and information, in possession of the Service Provider pertaining to Pioneer and/or any other asset of Pioneer.

- **Termination of Agreement:**

Both the parties shall have right to terminate the agreement as per the terms agreed between the Parties under the respective agreements. In case of any material breach of any of the terms & conditions of the agreement, the agreement shall be terminated with immediate effect at the option of the non-defaulting party and as more particularly mentioned under the respective agreements.