Policy on Outsourcing Financial Services & IT Services

And Code of Conduct for Direct Sales Agent (DSA)/Direct Marketing Agents (DMA)

and Recovery Agents

Of

FDPL FINANCE PRIVATE LIMITED

(FFPL)

Version	Approval Date	Version History	Approval Authority
I	12-Dec-23	FPCFY24-01	Board of Directors
II	15-Jan-25	FFCFY25-01	Board of Directors
III	08-Jan-26	FFCFY26-01	Board of Directors

Index

Introduction

Outsourcing is an arrangement whereby FDPL Finance Private Limited (the Company/NBFC) will use a third party (either an affiliated entity within the group or an entity that is external to the group) to perform activities continuously that would normally be undertaken by the Company itself, now or in the future. This includes arrangements for a limited period.

This policy contains the criteria for selection of financial activities and IT Outsourcing that may be outsourced as well as service providers and the systems to be put in place to monitor and review the operation of outsourced activities. Additionally, we have a separate IT Sourced and Cloud Monitoring

Policy in place, which is also prepared in accordance with RBI IT Governance and RBI Outsourcing Directions.

This Policy is framed in accordance with the applicable provisions of the Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025, as amended from time to time, read together with the Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025, Reserve Bank of India (Non-Banking Financial Companies – Credit Facilities) Directions, 2025
and
Reserve Bank of India (Non-Banking Financial Companies – Responsible Business Conduct) Directions, 2025

This Policy has been approved by the Board of Directors. Any changes to this Policy would require approval of the Board.

A. Objectives of the Policy

The objectives of the Outsourcing Policy (the "Policy") are to

i. Provide effective oversight, due diligence, and risk management for outsourced financial and IT-related services.

ii. Safeguard data security and related aspects to protect the Company's brand value and support the achievement of its business objectives in a fair and secure manner

iii. Protect the interests and confidentiality of the Company's customers at all times

B. Key Principles

The key principles of the outsourcing policy are outlined below:

i. The Company would ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and the Reserve Bank of India (RBI) nor impede effective supervision by the RBI.
ii. The Company would ensure that the service provider employs the same high standards of care in performing the services as would be employed by the Company itself. Accordingly, the Company would not engage in outsourcing its activities that would result in its internal control, business conduct or reputation being compromised or weakened.
iii. The Company would retain ultimate control of the outsourced activity. While outsourcing any activity, the Company would ensure that it has access to all relevant records and information available with the service provider.
iv. The grievance redressal mechanism in the Company would not, in any way, be compromised on account of outsourcing.
v. The Company would ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.
vi. The Board of Directors would have the ultimate responsibility for the outsourced activity.
vii. The Policy will be reviewed on an annual basis.

C. Indicative List of Activities that can be outsourced

The guidelines contained in this Policy are applicable to material outsourcing arrangements entered into by the Company with a service provider located in India or elsewhere. The service provider may either be a group company or an unrelated party.

An indicative list of activities that may be considered for outsourcing is as under:

i. Application processing (loan origination)
ii. Document processing
iii. Storage of documents
iv. Research and marketing
v. Supervision of loans
vi. Collection
vii. Recovery and repossession
viii. Data processing
ix. Other Back office related activities
x. Lead sourcing activity
xi. Field Investigation
xii. Marketing Campaigns

D. Activities that cannot be outsourced

In conformity with RBI guidelines, the Company shall not outsource core management functions including:

(i) Strategic and decision-making functions such as underwriting and sanctioning of loans
(ii) Internal Audit (Internal auditors can be appointed on a contract basis)
(iii) Management of investment portfolio
(iv) Functions such as determining compliance with KYC norms for opening accounts.

E. Outsourcing Digital Platforms

In case the Company lends through outsourced lending platforms, it would adhere to the Fair Practices Code in letter and spirit, also the guidelines laid down in this Policy. Wherever the Company engages digital lending platforms as its agents to source borrowers and/ or to recover dues, it would adhere to the following:

i. Names of digital lending platforms engaged as agents shall be disclosed on the Company's website.
ii. Digital lending platforms engaged as agents would be directed to disclose upfront to the customer that they are acting on behalf of the Company.
iii. Any outsourcing agreement entered by an NBFC with an LSP shall in no manner dilute or absolve the NBFC of its obligations under any statutory or regulatory provision.
iv. The Company shall issue a sanction letter / KFS to the borrower on its letterhead, immediately after sanction but before execution of the loan agreement.
v. A copy of the loan agreement along with a copy of each of all enclosures quoted in the loan agreement would be furnished to all borrowers at the time of sanction/ disbursement of loans.
vi. The Company would ensure effective oversight and monitoring over the digital lending platforms whose services are engaged.
vii. The Company would ensure that adequate efforts are made towards creation of awareness about the grievance redressal mechanism.

F. Role of the Board, Senior Management

Governance	Responsibilities
Board of Directors or a Committee of the Board	**Responsible for** i. The effective management and oversight of the outsourcing arrangement ii. Undertake regular review of outsourcing strategies & arrangements for their continued relevance, safety & soundness iii. Decide on business activities of a material nature to be outsourced and approve such agreements iv. Monitor the system of internal audit of outsourced activities and review ageing analysis of entries pending reconciliation with outsourced vendors v. Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements vi. Approving a policy for outsourcing financial services to a group entity
Senior Management	**Responsible for** i. Evaluate the risks and materiality of all existing and prospective outsourcing, based on the framework approved by the Board ii. Develop and implement sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing activity iii. Review of outsourcing arrangements to identify material risks iv. Periodically review the effectiveness of policies and procedures v. Ensuring that contingency plans are in place and tested vi. Ensure that there is independent review and audit for compliance with set policies
Risk Management Committee	**Responsible:** I. The Board of Directors shall review the records of all material outsourcing arrangements on a half-yearly basis. Where the Board delegates such review, the delegation shall be only to the Risk Management Committee of the Board, in accordance with applicable RBI Directions II. Ensuring that the Service Provider, if not a group company, shall not be owned or controlled by any director, key managerial personnel, approver of the Outsourcing arrangement, or their relatives. Audit Committee

G. Evaluation of Materiality

Material outsourcing arrangements are those which, if disrupted, have the potential to significantly impact the business operations, reputation or profitability. To evaluate the materiality of the outsourcing arrangement, the Company will consider the following aspects:

i. The level of importance of the activity being outsourced.

ii. Potential impact of the outsourcing on the Company on various parameters such as earnings, solvency, liquidity, funding capital and risk profile.
iii. The likely impact on the Company's reputation and brand value and ability to achieve its business objectives, strategy and plans, if the service provider fails to perform the service.
iv. The cost of outsourcing as a proportion of total operating costs of the Company.
v. The aggregate exposure to a particular service provider, in cases where the Company outsources various functions to the same service provider.
vi. The significance of activities outsourced in the context of customer service and protection.

H. Evaluation of Capability of the Service Provider

Capabilities of the service provider shall be assessed on the following parameters (indicative list):

i. Expertise, Vintage of operations of the Service Provider handling the relevant business
ii. The Service Provider's business reputation and track record in undertaking similar work in the recent past and competence to implement and support the proposed activity over the contracted period
iii. Financial soundness and ability to meet service commitments even under adverse conditions
iv. Track record of compliance and outstanding or potential litigations
v. Where possible, the Company would obtain independent reviews and market feedback on the service provider to supplement its own findings.
vi. The Company would ensure that the service providers' systems are compatible with that of its own and their standard of performance including in the area of customer service is also acceptable to the Company.
vii. The Company would also consider if there is undue concentration of outsourcing arrangements with a single service provider.
viii. The service provider, if not a group company, shall not be owned or controlled by any director of the Company or their relatives.
ix. In considering renewal of an outsourcing arrangement, shall perform appropriate due diligence to assess the capability of the Service Provider to comply with obligations in the outsourcing agreement.

I. The Outsourcing Agreement

The terms and conditions governing the contract between the Company and the service provider would be carefully defined in the agreement and vetted by the Company's legal counsel on their legal effect and enforceability.

The agreement would, inter alia, contain the following provisions:
The activities proposed to be outsourced, including the appropriate service and performance standards.

i. Risks and risk mitigation strategies.
ii. Continuous monitoring and assessment by the company of the service provider so that any necessary corrective measures could be taken immediately.
iii. Contingency plans to ensure business continuity. An appropriate level of control and right to intervene with appropriate measures to continue the business operations of the Company without incurring prohibitive expenses and without any break in services to the customers of the Company;
iv. A notice period in order to mitigate the risk of unexpected termination thereof or liquidation of the Service Provider.
v. Provision relating to prior approval / consent by the company for use of sub-contractors by the service provider for all or any part of an outsourced activity.
vi. A provision to the effect 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;
vii. A clause allowing 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.

viii. A clause to recognize the right of RBI to cause an inspection to be made of a service provider of the company and its books and accounts by officials of RBI or other authorised persons.
ix. Dispute resolution process, including events of default, and the indemnities, remedies and recourse of the respective parties.
x. Clauses relating to default, termination (including the minimum period to execute a termination provision) and early exit to allow the Company to terminate the agreement.
xi. Controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.
xii. A provision to the effect that confidentiality of customer's required information would be maintained even after the contract expires or gets terminated.
xiii. Provision relating to preservation of documents and data by the service provider in accordance with the legal/regulatory obligations of the Company.
xiv. Right of the Company 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.
xv. The Agreement would be sufficiently flexible so as allow the Company to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet legal and regulatory obligations.

J. Confidentiality and Security

Confidentiality of customer information is a pre-requisite for the stability and reputation of the Company, and therefore, the Company shall ensure that:

i. Access to customer information by the staff of the service provider would be on a "need to know" basis, i.e., limited to those areas where the information is required to perform the outsourced function.
ii. Any information disclosed should be used strictly for the purpose for which they were disclosed by the Company.
iii. The Company would review and monitor the security practices and control processes of the service provider regularly and require the service provider to disclose security breaches.
iv. The Company would ensure that the service provider can isolate and clearly identify the Company's customer information, documents and records to protect the confidentiality of the information. If the service provider acts as an outsourcing agent for multiple NBFCs / Banks, care would be taken to build strong safeguards so that there is no co-mingling of information/ documents and records.
v. The Company would immediately notify RBI in the event of any breach of security and leakage of confidential customer-related information.

K. Risks in Outsourcing

Outsourcing activities to third parties carry certain inherent risks. Failure in providing a specified service, breach in security/confidentiality or non-compliance with legal and regulatory requirements by the service provider may lead to financial and reputational losses for the organization. Therefore, the organization shall ensure effective evaluation and management of the following risks associated with outsourcing risk:

i. **Strategic Risk:** The service provider may conduct operations which are inconsistent with the overall strategic goals of the Company. Loss of relevant skills in the Company may prevent it from bringing the outsourced activity back in the Company.
ii. **Reputation Risk:** Risk of loss of the Company's reputation when the service delivered by the service provider is of poor quality and is not consistent with the standards of the Company.
iii. **Compliance Risk:** Privacy, consumer and prudential guidelines not adequately complied with.
iv. **Operational Risk:** Risk arising from technology failure, fraud and error, lack of adequate financial capacity of the service provider to fulfil obligations or provide remedies for such inadequacy.
v. **Legal Risk:** This includes but is not limited to exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the service provider.

vi. **Exit Strategy Risk:** This could arise from over-reliance on one firm and contracts entered into wherein speedy exits would be prohibitively expensive.
vii. **Counterparty Risk:** Risk arising out of inappropriate underwriting or credit assessments.
viii. **Country Risk:** Risk arising out of any significant change in political, social, or legal climate.
ix. **Contractual Risk:** Risk arising out of legal gaps in the contract, wherein the company is not able to enforce the contract on the service provider
x. **Concentration and Systemic Risk:** Where there is a lack of control of an NBFC over a service provider, more so when the overall industry has considerable exposure to one service provider

L. Responsibilities of Direct Sales Agents (DSA) / Direct Marketing Agents (DMA) /

I. The Direct Sales Agents (DSA)/ Direct Marketing Agents (DMA)/ Recovery Agents (RA) engaged by the Company shall not resort to:
   a) intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts;
   b) acts intended to humiliate publicly or intrude on the privacy of the debtors' family members, referees and friends;
   c) making threatening and anonymous calls; or
   d) making false and misleading representations.

II. The Company would ensure that the DSA/ DMA / Recovery Agents 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.

III. The Company would put in place a Board-approved Code of Conduct for DSA/DMA/ Recovery Agents and obtain their undertaking to abide by the Code.

IV. The Recovery Agents would adhere to the extant instructions on the Fair Practices Code adopted by the Company for collection of dues and repossession of security.

M. Business Continuity and Management of Disaster Recovery Plan

i. The Company shall require its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures.
ii. The Company would ensure that the Service Provider regularly tests the Business Continuity and Disaster Recovery Plan. The Company would also conduct occasional joint testing and recovery exercises with the Service Provider.
iii. The Company would ensure that alternative Service Providers are available or there is a possibility of bringing the outsourced activity back in-house in case of emergency.
iv. The Company would ensure that the service provider is able to isolate the Company's information, documents and records. This will enable the Company, in appropriate situations, to retrieve all documents and information given to the service provider in order to continue its business.

N. Monitoring of Outsourced Activities

i. A central record of all material outsourcing, that is readily accessible for review by the Board and senior management of the Company, would be maintained. The records would be updated promptly and half-yearly reviews would be placed before the Board of Directors or risk management committee
ii. Regular audits would be undertaken by either the internal auditors or external auditors of the Company to assess the adequacy of risk management practices adopted in overseeing and managing the outsourcing arrangement. The observations of the auditors would be placed before the Board of Directors.
iii. The Company would review the financial and operational condition of the service provider annually. The purpose of this review would be to assess the service provider's ability to continue to meet the outsourcing obligations and identify any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

iv. In the event of termination of an outsourcing agreement, in cases where the service provider deals with customers, the same would be publicized by displaying at a prominent place in the Company's office, posting it on the website and informing the customers to ensure that the customers do not continue to deal with the said service provider.
v. Certain cases, like outsourcing of cash management, might involve reconciliation of transactions between the Company, the service provider and its sub-contractors. In such cases, the Company will ensure that timely reconciliation of transactions with the service provider (and/ or its subcontractor), are carried out in a timely manner. An ageing analysis of entries pending reconciliation with outsourced vendors shall be reviewed by the Finance Controller and the Company shall make efforts to reduce the old outstanding items therein at the earliest.
vi. The Company would put in place a robust system of internal audit of all outsourced activities, which would be monitored by its Finance Controller.

O. Redressal of Grievances related to Outsourced Services

The grievance redressal mechanism, as laid down in the Fair Practices Code and the Grievance Redressal Policy, would also apply to issues related to services provided by outsourced agencies.

P. Reporting of transactions to Financial Intelligence Unit (FIU) or other competent authorities

The Company would submit Currency Transactions Reports and Suspicious Transactions Reports, if any, to FIU or any other competent authority in respect of the Company's customer-related activities carried out by the Service Providers.

Q. Outsourcing to a Group Entity

In case of outsourcing any activity within the group companies, the Company shall ensure that:

i. Arm's length distance is maintained in such outsourcing in terms of premises, manpower, decision-making, record keeping, etc. for avoidance of potential conflict of interests between the Company and such Service Provider and accordingly necessary disclosures in this regard shall be made as part of the outsourcing agreement;
ii. The customers are informed specifically about the company which is actually offering the product/ service in case of involvement of multiple group entities involved or cross-selling of products;
iii. The outsourcing agreement would address the provisions including scope of services, charges for the services and maintaining confidentiality of the customer's data;
iv. The arrangement shall not lead to any confusion to the customers as to 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;
v. The arrangement shall not compromise the ability to identify and manage risk of the Company on a stand-alone basis;
vi. The arrangement shall not prevent RBI from being able to obtain information required for the supervision of the Company or pertaining to the group as a whole;
vii. The Company's ability to carry out its operations in a sound fashion would not be affected if premises or other services (such as IT systems, support staff) provided by the group entities become unavailable;
viii. If the premises of the Company are shared with group entities, the Company will ensure that its identification is distinctly visible to the customers.
ix. The marketing brochure used by the group entity and verbal communication by its staff/ agent in the Company's premises shall mention the nature of arrangement of the entity with the Company so that the customers are clear on the seller of the product.
x. The risk management practices expected to be adopted by the Company while outsourcing to a related party (i.e. party within the Group/ Conglomerate) would be identical to those specified with respect to other service providers in this Policy.

xi. (xi) The Company shall not publish any advertisement or enter into any agreement stating or suggesting or giving tacit impression that it is responsible for the obligations of its group entities."

R. Off-shore outsourcing of financial services

In case of offshore outsourcing of financial services, particularly relating to Indian Operations, the Company shall ensure that:

i. The Company takes into account and closely monitors the government policies and political, social, economic and legal conditions in the countries where the Service Provider is based, both during the risk assessment process and on a continuous basis and establish sound procedures for dealing with country risk problems. The Company would have in place appropriate contingency and exit strategies.
ii. Such arrangements would be entered into only with the parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified in the agreement.
iii. The outsourced activities are conducted in a manner so as not to hinder the efforts to supervise or reconstruct the Indian activities of the Company in a timely manner.
iv. Where the off-shore Service Provider is a regulated entity, the relevant off-shore regulator will neither obstruct the arrangement nor object to inspection visits of RBI or visits of the Company's internal and external auditors.
v. The availability of records to management and RBI will withstand the liquidation of either the offshore custodian or the Company in India.
vi. The regulatory authority of the offshore location does not have access to the data relating to Indian operations of the Company simply on the ground that the processing is being undertaken there.
vii. The jurisdiction of the courts in the off-shore location where data is maintained does not extend to operations of the Company in India on the strength of the fact that the data is being processed there even though the actual transactions are undertaken in India.
viii. All original records will be maintained in India.

S. Review Frequency

This Policy shall be reviewed at regular intervals or as and when considered necessary by the Board of Directors/Committee of the Company.

T. Code Of Conduct for Recovery Agents / Collection Agencies

All the members/staff/agents/contractors/subcontractors of the Service Provider ("Personnel") collecting any due amounts from the Borrower on behalf of the Company shall at all times follow the guidelines set out herein below:

1. Borrowers should be contacted ordinarily at the place of their choice and in the absence of any specified place, at the place of their residence.
2. Identity and authority of the Personnel should be made known to the Borrower at the first instance when contacting them digitally / telephonically / or physically. Further, details of the grievance redressal mechanism in case of any complaint for misbehavior shall be communicated to the Borrower
3. Borrower's privacy should be respected. When the Personnel calls the Borrower, they shall record the time of calls and content of the calls and maintain clear, concise and accurate records on the same day. At the beginning of each call, after the introduction, the Personnel shall inform the Borrower that the call is being recorded for quality assurance and training purposes.
4. Interaction with the Borrower should be in a civil manner. Borrower should be contacted between 08:00 hrs and 19:00 hrs, unless the special circumstance of the Borrower 's business or occupation requires otherwise, and such special circumstance has been specified by the Borrower. In such an event, the

Borrower shall be contacted as per the timings requested by the Borrower. Personnel shall ensure that such communication from the Borrower is duly recorded for review and verification by the Company failing which the Service Provider shall be deemed to be in breach of this obligation. The Personnel shall contact the Borrower for a maximum of 5 times in a day through calls/aut dialers.

5. Borrower's request to avoid calls at a particular time or at a particular place should be honored as far as possible.
6. Time and number of calls and contents of conversation should be documented. The Personnel of the Service Provider shall document the disposition/details of the attempt to contact. The records should be clear, concise, accurate and free of editorial comments.
7. Cases with unresolved issues shall be escalated to the immediate supervisor. Borrower or third-party requests to speak with the immediate supervisor should be honored if the Borrower is not satisfied with the actions of the Personnel.
8. Borrower should be provided with all the information regarding any outstanding dues with respect to the Credit Facility availed by them and necessary notice should be given for enabling discharge of such outstanding dues.
9. Reasonable notice would be given before repossession of security and its realization.
10. All assistance should be given to resolve disputes or differences in a mutually acceptable and in an ordinary manner.
11. During visit to the Borrower's place for collection of any due amount, decency and decorum should be maintained.
12. Inappropriate occasions such as, bereavement in the family or such other calamitous occasions should be avoided for making calls/visits to collect dues.
13. Demeanor that would suggest criminal intimidation or threat of violence should be carefully avoided. The personnel shall only use acceptable business language, even if the Borrower does not. If the borrower shows abusive or threatening behaviour or signs of stress, the recovery personnel must bring it to the notice of their senior manager and document it appropriately and immediately.
14. Service Provider and its Personnel, while collecting the amount due, should not resort to any false, deceptive or misleading representation. It should not falsely represent or imply that the Service Provider or its Personnel is connected with or affiliated with any governmental or judicial authority and shall abstain from using any identification which can lead to wrong representation. The Service Provider or its Personnel should also not falsely represent the character, amount, or legal status of the Credit Facility availed by the Borrower. In case of non-adherence to the above terms, the Service Provider will be solely responsible for any and every consequence arising thereof.
15. If the Borrower refuses to pay, the Personnel must understand the reason of such a refusal and efforts should be made to explain the consequences to the Borrower, including but not limited to, the impact on credit history of the Borrower, possible legal action and its impact on the Borrower, cost of defending legal action, if such action is contemplated.
16. The Personnel shall not give any commitment whatsoever concerning waivers, discounts, extension of time period for payment of dues etc. with respect to a Credit Facility, to the defaulting Borrowers without prior written consent from the Company.
17. Personnel shall not accept inducements or gifts from the borrower; if any are offered, the employee or agent should bring them to the attention of his/her immediate supervisor.
18. Personnel shall answer the borrower's questions in full, including payment details, penalties, and waivers if within the permitted parameters. They shall flag the unresolved questions with the senior management as necessary and follow-up on the verbal communication with written feedback.
19. The recovery payments form the Borrower shall not be credited to the recovery agent or any other account.

T.1 CUSTOMER COMMUNICATION GUIDELINES

The following guidelines are to be complied with along with the Code of Conduct by the Service Provider and its Personnel who are authorized to represent the Company in the collection of outstanding dues with respect to a Credit Facility from the Borrower.

1. Borrowers shall be treated with dignity. During all conversations with the Borrower, over telephone, in writing or during visits, professionalism and transparency will be ensured.
2. Personnel shall be polite, professional and well-behaved and should try to use the language which the Borrower understands and formal mode of address in the language of Borrower's choice should be used. Use of tough or aggressive or threatening or abusive language, either verbal or in writing should not be made. Care should be taken not to threaten/harass/torment the Borrower in any manner.
3. Service Provider are required to inform the Company of the Borrowers who become abusive or threatening. All such instances should be appropriately documented.
4. Service Provider and its Personnel shall not promise or commit for any type of written communication on behalf of the Company. Further, they should not send any other written communication via email, letter or social media to the Borrowers unless approved by the Company in writing.
5. Service Provider and its Personnel shall not mislead the Borrower and/or induce any bribes or payments from the Borrower.
6. Personnel shall not mislead the Borrower about their true business or organization name.
7. Communications with Borrowers must go through designated company channels for calls, SMS and emails. Personnel shall not use their personal phones / emails / devices for recovery purposes. Further, all the communications shall be conducted in designated formats approved by the quality check / control department.

U. Code of Conduct For Direct Sales Agent (DSA)/Direct Marketing Agents (DMA)

U.1 Applicability

This Code of Conduct for DSA/DMA is for adoption and implementation by DSA/DMA while acting as agents/employees of the Company. This Code will apply to all persons involved in sales/distribution of any product/service of the Company. All DSAs/DMAs and telemarketing executives, field sales personnel, business development executives, employees, representatives, and all persons must agree to abide by this code prior.

U.2 Compliance with Telemarketing Regulations

The Company shall engage only those Direct Sales Agents (DSAs) / Direct Marketing Agents (DMAs) acting as telemarketers who possess valid registration with the Department of Telecommunications (DoT) and comply with the guidelines issued by Telecom Regulatory Authority of India (TRAI) from time to time.
The Company shall maintain and furnish the list of telemarketers and registered telephone numbers used for telemarketing activities to TRAI, wherever required.
The Company shall ensure that all telemarketing agents engaged by it remain duly registered with DoT at all times.

U.3 Every DSA/DMA shall adhere to the code of conduct specified below:

a) No misleading statements/misrepresentations permitted
b) DSA/DMA should not -
- Mislead the Customer/Borrower on any service / Loan Product offered;
- Mislead the Customer/Borrower about their business or organization's name, or falsely represent themselves;

- Make any false/unauthorized commitment on behalf of the Company for any Credit Facility/Loan Product.

c) Gifts or bribes/Kickbacks:

DSA/DMA must not accept gifts from Customers/Borrowers or bribes/kickbacks whether in cash or kind. Any DSA/DMA offered a bribe or payment of any kind by a Customer/Borrower must report the offer to his/her management and the Company.

d) Handling of letters & other communication:

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

e) DSA/DMA shall not:

- Induce the Customer to omit any material information in the proposal/application form
- Induce the Customer to submit wrong information in the proposal form or documents submitted to the Company for evaluation
- Behave in a discourteous manner with the Customer

f) DSA/DMA shall:

- Be responsible for all acts of omission and commission of its personnel
- Ensure that all its personnel are properly trained, skilled and knowledgeable in the Loan Products they market
- Take appropriate steps to maintain the security of confidential documents of Borrowers/Customers in their possession;
- Be Compliant with Business Continuity Plan (BCP) norms as required by the Company from time to time
- Ensure confidentiality of Borrower/Customer data and shall not disclose to any third party without the consent of Borrower.
- Adhere and comply with all the processes & procedures laid down by the Company

g) Telemarketing etiquettes for DSAS/DMAs and their personnel/agents

- Pre-call:
  - (a) No calls prior to 0930 Hrs or post 1900 Hrs unless specifically requested.
  - (b) No calling on lists unless the list is cleared by a team leader.
  - (c) No calling a person who has been flagged in any “Do Not Call” list

- During Call:
  - (a) Identify himself/herself, his/her company and request permission to proceed from the Customer.
  - (b) If denied permission, must apologize and politely disconnect. He/she should state the reason for the call.
  - (c) must always offer to call back on landline, if call is made to a cell number, and never interrupt or argue.
  - (d) To the extent possible, must talk in the language, which is most comfortable to the Customer, and keep the conversation limited to business matters.
  - (e) must check for understanding of “Most Important Terms and Conditions” by the Customer if he/she plans to avail the Loan Product.
  - (f) must reconfirm next call or next visit details.
  - (g) must provide his/her telephone number, supervisor’s name or Company’s contact details if asked for by the Customer.

- Post Call:
  (a) Customers who have expressed their lack of interest for the offering should not be called for the next 3 months with the same offer, unless they express interest.
  (b) Provide feedback to Company on Customers who have expressed their desire to be flagged "Do Not Disturb".
  (c) Never call or entertain calls from Customers regarding Loan Products already sold and must always advise them to contact the Company.

V. Exit Strategy

i. All agreements with Service Providers shall include a termination clause, with a minimum notice period for execution of the exit plan as defined in the agreement, ensuring sufficient time for transition activities. This period shall be established based on the complexity of the Outsourced Services and contractual obligations, in line with the Company's Contractual Policy.
ii. Prior to termination of the Outsourcing agreement, the department concerned shall identify alternative arrangements to ensure business continuity, which may include engaging a different Service Provider or reassigning the activity to internal resources within FFPL.
iii. The Company shall ensure that outsourcing agreements have necessary clauses on safe removal or destruction of data, hardware and all records (digital and physical), as applicable. Further, the outsourcing agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering, or changing any data during the transition period, unless specifically advised by the regulator or FFPL
iv. The service provider shall be legally obligated to fully cooperate with both FFPL and any new service provider(s), through an agreement, to ensure a seamless transition of services.
v. The IT Outsourcing agreement shall ensure further that the service provider is prohibited from erasing, purging, revoking, altering, or changing any data during the transition period, unless specifically advised by the RBI or FFPL.

A. IT SERVICES OUTSOURCING POLICY

1. IT Services Outsourcing Framework

The Company shall ensure that all Information Technology outsourcing arrangements are aligned with its strategic objectives and are supported by appropriate governance, risk management, information security and oversight mechanisms.

Prior to entering into any outsourcing arrangement, the Company shall assess the associated risks, contractual obligations, information security implications and regulatory requirements.

The Company shall classify outsourced Information Technology services based on their materiality and criticality with reference to business operations, customer impact, information security, regulatory compliance and operational resilience. The level of oversight, monitoring, approval and control shall be commensurate with the materiality of the outsourced service.

2. Material Outsourcing of IT Services

An outsourcing arrangement shall be considered material where disruption, failure, compromise or unavailability of the outsourced service may have a significant impact on the Company's business operations, customer service, information security, regulatory compliance or operational resilience.

Materiality shall be assessed considering, among other factors:

- the importance of the service to business operations;
- the potential impact on customers due to loss, theft or unauthorised access to information;
- the impact on regulatory compliance;
- the effect on operational resilience, business continuity and disaster recovery capabilities; and
- the extent of dependency on the service provider.

Examples of material IT outsourcing may include cloud computing services, data centre services, managed security services, application development and maintenance, network and security operations, and payment technology infrastructure.

3. Outsourcing Agreements

All Information Technology outsourcing arrangements shall be governed by written agreements that clearly define the rights, obligations and responsibilities of the Company and the service provider.

The agreements shall be reviewed by the Company's legal counsel to ensure their legal validity and enforceability.

The outsourcing agreement shall, as applicable, include provisions relating to the scope of services, service level agreements, performance standards, audit and inspection rights, access rights of the Company and the Reserve Bank of India, approval requirements for subcontracting, confidentiality and data protection obligations, incident reporting requirements, data location requirements applicable to the Company, business continuity and disaster recovery obligations, termination rights, transition support, return of data, secure destruction of data, liability of the service provider for its subcontractors, and compliance with applicable RBI directions and legal requirements.

The agreement shall be sufficiently flexible to enable the Company to retain an appropriate level of control over the outsourced activity and to take necessary measures to meet its legal and regulatory obligations.

4. Audit, Inspection & Access Rights

The Company shall retain the right to access books, records, audit trails, logs, systems, premises and other information relating to outsourced activities, subject to applicable security protocols.

The Company shall have the right to conduct audits of outsourced service providers, either directly or through internal or external auditors appointed on its behalf.

Where required under applicable regulations, the outsourcing agreement shall provide the Reserve Bank of India or its authorised representatives with access to records, documents, systems and information maintained by the outsourced service provider and its material subcontractors.

5. Board & Senior Management Responsibilities

The Board of Directors and Senior Management shall remain ultimately responsible for all outsourced Information Technology operations.

The Board shall approve the Information Technology outsourcing policy, establish an appropriate governance framework, define approval authorities based on risk and materiality, and periodically review material outsourcing arrangements and significant outsourcing risks.

Senior Management shall be responsible for implementing the approved policy, evaluating risks of existing and proposed outsourcing arrangements, ensuring effective oversight of service providers, monitoring outsourcing-related risks, ensuring business continuity preparedness and reporting significant issues to the Board or the appropriate Committee of the Board.
@ww

Outsourcing of Information Technology services shall not diminish the Company's obligations to its customers, regulators or other stakeholders.

6. Risk Assessment & Concentration Risk

A documented risk assessment shall be conducted before onboarding any outsourced Information Technology service provider.

The assessment shall cover operational, cyber security, legal, compliance, financial, reputational, concentration and exit risks associated with the outsourcing arrangement.

The Company shall assess concentration risk arising from dependence on a single service provider or a limited number of service providers for critical or material services.

Risk assessments shall be reviewed periodically and updated whenever there are significant changes in the outsourcing arrangement, technology environment, business operations or regulatory requirements.

7. Service Provider Due Diligence

The Company shall conduct appropriate due diligence before entering into or renewing an outsourcing arrangement.

Due diligence shall include assessment of the service provider's financial stability, technical capability, information security controls, backup and disaster recovery capability, data segregation capability, compliance with applicable laws and RBI requirements, governance over subcontractors, business reputation, past security incidents and litigation history, and ability to provide the services on an ongoing basis.

The extent of due diligence shall be proportionate to the materiality and risk of the outsourced service.

8. Information Security & Data Protection

The Company shall retain ownership of all data, information and technology assets processed, stored or managed by the service provider on behalf of the Company.

Access to Company data shall be provided strictly on a need-to-know basis and shall be subject to appropriate authentication, authorisation and monitoring controls.

The service provider shall implement appropriate encryption, logical segregation and security controls to protect the confidentiality, integrity and availability of Company data.

In multi-tenant cloud or shared environments, the service provider shall ensure clear isolation of the Company's data from that of other customers.

The service provider shall notify the Company of any actual or suspected security breach, data leakage, unauthorised access or compromise without undue delay.

The outsourcing arrangement shall comply with the Company's information security requirements, contractual obligations and applicable regulatory requirements.

9. Cyber Incident Reporting

Service providers shall notify the Company immediately upon detection of any cyber incident, security breach, service unavailability, denial-of-service event, ransomware incident, malware outbreak, unauthorised access or any other event affecting the outsourced service or Company data.

The Company shall establish appropriate procedures for assessment, escalation, response, recovery and regulatory reporting of such incidents in accordance with applicable internal policies and regulatory requirements.

10. Subcontracting

Material subcontracting of outsourced Information Technology services shall require the prior written approval of the Company.

The service provider shall ensure that all security, confidentiality, compliance, audit and business continuity obligations applicable to the primary outsourcing arrangement are contractually flowed down to the subcontractor.

The service provider shall remain fully responsible and accountable for the acts, omissions, performance and security posture of its subcontractors.

11. Exit Strategy & Termination

The Company shall maintain a documented exit strategy for all material Information Technology outsourcing arrangements to ensure business continuity during and after termination or exit.

The exit strategy shall include transition planning, minimum transition periods, migration assistance, return of data and assets, secure deletion of data, transfer of knowledge and cooperation with replacement service providers.

The outsourcing agreement shall prohibit the service provider from altering, deleting, revoking or purging Company data during the transition period unless specifically authorised by the Company or required by law or regulation.

12. Outsourcing Security Operations Centre (SOC)

Where the Company outsources Security Operations Centre (SOC) operations, the arrangement shall be subject to enhanced governance, security and oversight controls commensurate with the criticality of the outsourced SOC services.

The Company shall ensure that ownership of information assets, security logs, configurations, rules, analytics, alerts and incident records relating to the Company remains clearly identified and under the control of the Company.

The Company shall maintain adequate oversight over the definition, customization, review and approval of security monitoring rules, use cases and detection mechanisms applicable to the Company's environment.

The outsourced SOC reporting, escalation and incident handling process shall be integrated with the Company's incident response and cyber security management framework to ensure timely detection, assessment, escalation, containment, recovery and reporting of security incidents.

The Company may periodically assess the effectiveness of the outsourced SOC operations, including the security controls, operational processes, physical facilities involved in service delivery, handling of alerts and events, and compliance with contractual and regulatory requirements.

The service provider shall ensure that access to security logs, alerts, monitoring tools and related data is restricted to authorized personnel and is subject to appropriate confidentiality, integrity and audit controls.

13. Cloud Computing Services

Cloud computing services shall be subject to enhanced risk assessment and governance controls.

The Company shall ensure that cloud service providers support appropriate identity and access management, multi-factor authentication, logging and monitoring, encryption, operational resilience, vendor oversight and exit management controls in accordance with the Company's cloud governance framework.

The use of cloud services shall be consistent with applicable RBI requirements and the Company's information security and cloud governance framework.

The Company shall also ensure that roles and responsibilities between the Company and the cloud service provider are appropriately defined and periodically reviewed.