BRMP LEASING & FINANCE PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC) AND

ANTI-MONEY LAUNDERING (AML) POLICY

RECORD OF REVIEW

BRMP LEASING AND FINANCE PRIVATE LIMITED	
Policy Title	Know Your Customer (KYC) And Anti-Money Laundering (AML) Policy
Created By	Compliance Department
Reviewing & Approving Authority	Board of Directors
Version No.	1
Date of approval	20-10-2025
Review Cycle	Annually or as recommended by the Board of Directors
Nature of Document	External

TABLE OF CONTENTS

1. INTRODUCTION

BRMP LEASING & FINANCE PRIVATE LIMITED ("the Company") is a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India (RBI) under the Non-Deposit Taking Base Layer category. The Company offers financial services to a diverse clientele, including individuals, MSMEs, entrepreneurs, and corporates.

2. REGULATORY REQUIREMENT

The "Know Your Customer" ("KYC") guidelines issued by the Reserve Bank Of India ("RBI") (RBI /DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016) as updated from time to time ("RBI KYC Guidelines")aims at preventing Non-Banking Finance Companies ("NBFCs") from being used intentionally or unintentionally by criminal elements for committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism. Accordingly, in compliance with the guidelines issued by RBI regularly, the Policy on Know Your Customer (KYC)/ Anti-Money Laundering (AML) ("Policy") of Company is hereby formulated and approved by its Board of Directors ("Board").

3. DEFINITION

Definitions in these Guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:-

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i) **"Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

ii) **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

iii) **"Authentication",** in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iv) **"Beneficial Owner" (BO):**

(a) Where the customer is a company, the BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.

For the purpose of this sub-clause: -

1) "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.

2) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

(b) Where the customer is a partnership firm, the BO is the natural person(s), who, whether alone or together, or through one or more juridical person, has / have ownership of entitlement acting to more than 15per cent of capital or profits of the partnership.

(c) Where the customer is an Unincorporated Association or 'Body of Individuals'**, the BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of entitlement to more than 15 per cent of the property or capital or profits of the Unincorporated Association or Body of Individuals.

Explanation: Term 'Body of Individuals' includes Societies

Where no natural person is identified under (a), (b) or (c) above, the BO is the relevant natural person who holds the position of Senior Managing Official.

(d) Where the customer is a trust, the identification of BO shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v) **"Certified Copy"** - Obtaining a certified copy by the company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the company as per the provisions contained in the Act.

vi) **"Central KYC Records Registry"** (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vii) **"Designated Director"** means the Managing Director or a whole-time Director, duly authorized by the Board of Directors of company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole

Time Director" shall have the meaning assigned to them in the Companies Act, 2013.

viii) **"Digital KYC"** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the company as per the provisions contained in the Act.

ix) **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

x) **"Equivalent e-document"** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016."Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry.

xi) **"Non-profit organisations" (NPO)** means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

xii) **"Officially Valid Document" (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address: -

   i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
   ii. property or Municipal tax receipt;
   iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
   iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official

accommodation;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.

d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xiii) **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xiv) **"Person"** has the same meaning as defined in the Act and includes: a) An individual, b) A Hindu undivided family, c) A company, d) A firm, e) An association of persons or a body of individuals, whether incorporated or not, f) Every artificial juridical person, not falling within anyone of the above persons (a to e), and g) Any agency, office or branch owned or controlled by any of the above persons (a to f).

xv) **"Principal Officer"** means an officer nominated by the company, responsible for furnishing information as per rule 8 of the Rules.

xvi) **"Suspicious Transaction" means** a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith: a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or b. appears to be made in circumstances of unusual or unjustified complexity; or c. appears to not have economic rationale or bona-fide purpose; or d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

xvii) **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of borrower's loan account;
b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether

in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. establishing or creating a legal person or legal arrangement.

xviii) **"Video based Customer Identification Process (V-CIP)":** a method of customer identification by an official of company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of these guidelines.

b) Terms bearing meaning assigned in these guidelines, unless the context otherwise requires, shall bear the meanings assigned to them below:

i) **"Customer"** means a person who is engaged in a financial transaction or activity with company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
For the purpose of this Policy, a "customer" will include the following:
   a) A person or entity who is engaged in financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting (i.e., the beneficial owner);
   b) Beneficiaries of transactions conducted by professional intermediaries such as Stock- brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law; or
   c) Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company. e.g., a wire transfer or issue of a high value demand draft as a single transaction.
   d) A past as well as prospective customer having attempted or executed transactions.

ii) **"Customer Acceptance Policy"** shall have the same meaning as specified in **clause 8** of this Policy.

iii) **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner.

iv) **"Customer identification"** means undertaking the process of CDD.

v) **"Know Your Customer Identifier"** means the unique number or code assigned to a client by the Central KYC Records Registry.

vi) **"Know Your Customer Records"** means all records, documents and information constituting the basis for caring out the Customer Due Diligence procedures in

accordance with Rule 9 of the Rules.

vii) **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

viii) **"Last KYC verification or updation"** means last transaction made in the CKYC records registry by which the KYC records of a customer where recorded, changed or updated

ix) **"Money Laundering"** shall have the same meaning as defined under section 3 of the Prevention of Money - laundering Act, 2002 for the time being in force.

x) **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

xi) **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

xii) **"Periodic Updation"** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xiii) **"Politically Exposed Persons"** (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/important political party officials, etc.

xiv) **"Regulated Entities"** (REs) means:

a) All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'.
b) All India Financial Institutions (AIFIs)
c) All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).
d) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers).
e) All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
f) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers).
g) All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

h) All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. PURPOSE

The purpose of the KYC and AML policy of the company is to ensure that the company understands/knows its customers and their transactions and to have a system to keep in check the money laundering activities.

The policy has been framed:
• To ensure compliance with the applicable rules and regulations;
• To obtain an understanding of the customer and transactions undertaken by them;
• To ensure that there is a customer acceptance and identification mechanism;
• To put in place appropriate controls to identify suspicious transactions and enable their timely reporting;

5. SCOPE OF THE POLICY

The provisions of KYC and AML policy shall apply to all the branches/offices of the company.

For the purpose of this policy, 'Customer' means a person who is engaged in a financial transaction or activity with the company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

In terms of PML Act a 'person' includes:
i. an individual,
ii. a Hindu undivided family,
iii. a company,
iv. a firm,
v. an association of persons or a body of individuals, whether incorporated or not,
vi. every artificial juridical person, not falling within any one of the above persons (i to v), and
vii. any agency, office or branch owned or controlled by any of the above persons (i to vi).

6. ROLES AND RESPONSIBILITIES

The Company's Board of Directors will oversee the implementation of KYC & AML norms and the management team is responsible for implementing the KYC & AML norms hereinafter detailed, and to Ensure That Its Operations Reflect Its Initiatives to Prevent Money-Laundering Activities.

7. KEY ELEMENTS OF KYC

KYC procedures also enable the Company to know/understand its Customers and their financial dealings better which in turn help to manage its risks prudently. We have framed the Policy incorporating the following five key elements:

- Customer Acceptance Policy **("CAP");**
- Risk management.
- Customer Identification Procedures **("CIP");**
- Customer Due Diligence Procedures **("CDD"); and**
- Risk Record Management **("RRM")** & Monitoring of transactions.

8. CUSTOMER ACCEPTANCE POLICY ("CAP")

The Company's CAP lays down criteria for acceptance of customers. The Company shall ensure that:

a. No account is opened in anonymous or fictitious benami name(s);
b. No account shall be opened where there is an inability to apply procedures for Customer Due Diligence either due to non-co-operation of the customer or non-reliability of the documents, records, information and explanation furnished by the customer.
c. No account based relationship shall be accepted without following the procedures as mandated in Rule 9 of the Rules.
d. Sufficient compliance with Rule 9 and appropriate KYC records shall be sort while accepting customer account based relationship.
e. Application of customer Due Diligence norms as per Rule 9 of the Rules at Global Customer ID level shall be undertaken while accepting customer account based relationship. However, no customer due diligence procedure shall be applied in case the existing KYC compliant customer desires to avail other services in addition to the first KYC compliant service.
f. In the case of joint accounts, separate customer due diligence procedures shall be undertaken for all the joint account holder in accordance with the Rule 9 of the Rules.
g. No service shall be denied to any customer on the ground that the customer does not have Aadhaar number in accordance with section 11 A(3) of the Act. In such a case, other KYC compliance procedure shall be observed.
h. Evaluate the circumstances in which the customer is permitted to act behalf of another

person or entity.

i. Suitable measures shall be stipulated for identification of customers whose name matches with the name of any person or entity notified under Chapter IX Master Direction – Know Your Customer (KYC) Direction, 2016.
j. Adequate steps shall be taken to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities such 9 as individual terrorists or terrorist organizations, sanctioned persons;
k. Verification of customer records such as PAN, GST registration certificates or any other equivalent e-documents shall be undertaken in accordance with the verification facilities provided by the issuing authorities as well as digital signatures as per the Information Technology Act, 2000.
l. Customer Acceptance Policy shall not result in denial of services to the general public especially those belonging to financially and socially disadvantaged individuals
m. If the Company is suspicious of money laundering or terrorist financing, and reasonably believes that performing the Customer Due Diligence (CDD) process will tip-off the customer, it shall not pursue the CDD process, and instead file a suspicious transaction report (STR) to FIU-IND.

In case of Inactive Prospective Customers (who do not approaches to the Company) the Company will auto-cancelled the case after 45 days of application creation date and data will store in the system. Application status will be mark as auto-cancelled.

9. RISK MANAGEMENT

The Company shall have risk based approach for management and mitigation of risk comprising the following:

1. The risk categorization of the customers shall be undertaken on the parameters such as customer's identity, occupation, social and financial status, location, nature of business activity, geographical risk covering customers as well as transaction, types of products and services offered and mode of payment as well as receipts.
2. While considering customer's identity, the ability to verify and confirm officially valid documents to the facilities providing by the issuing authorities shall also be taken into account.
3. Customers shall be categorized by low, medium and high risk based on the assessment and risk perception norms stipulated by the Company.
4. Broad principles shall be identified and stipulated for appropriate risk categorization of the customers. An indicative risk categorization for general guidance is provided in **Annexure I**.
5. The risk categorization of the customer and the specific reasons for such categorization shall be kept confidential, and shall never be revealed to any customer to avoid tipping off to any customer.

10. CUSTOMER IDENTIFICATION PROCEDURE ("CIP")

Customer identification procedures are made to ensure that the customers are identified by using reliable, independent source documents, data or information. The company should obtain information necessary to establish to its satisfaction the true identity of each customer and the purpose of the intended nature of companying relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers.

Customer identification is required in the below scenarios:

i. At the time of commencement of an account-based relationship with the customer i.e. on boarding of the customer.
ii. While carrying out financial transactions of the customer.
iii. If there is doubt or suspicion about the authenticity of the documents submitted by the customer for the purpose of his identification.
iv. When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.
v. When selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
vi. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
vii. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
viii. Maintain records of the information used to verify a customer's identity, including name, address and other identifying information.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the company, shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:

i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
ii. Adequate steps are taken to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
iii. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line

with the requirements and obligations under the PML Act.

iv. The third party shall not be based in a country or jurisdiction assessed as high risk.
v. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, is with the Company.

In order to complete the activity of customer identification, the company shall obtain information/documents from the customer at the time of on boarding or periodic updation. The type of documents to be collected would depend on the type of customer (individual, corporate, etc.)

While deciding the acceptable documents, the below factors have to be considered:

• The document should establish the legal status of the customer.

• The document should also establish the authority of the person, acting on behalf of the customer.

• The ultimate ownership of the legal entity should be established from the documents submitted. The beneficial owners who ultimately control the legal entity should be identifiable.

11.CUSTOMER PROFILE

For the purpose of exercising due diligence on individual transactions in accounts, a 'Customer Profile' of individual Customers is included in the loan application form. The customer profile will contain information relating to the Customer's identity, social/ financial status, information about the Customer's clients' business and their location etc. The information will be of two types namely mandatory and optional as stated below:

(a) Mandatory Information:
(i) Identity (ii) Address (iii) Occupation (iv) Source of funds (v) Monthly Income (vi) Annual turnover (vii) Date of Birth (viii) Assets (approximate value).
(b) Optional Information:
(i) Marital Status; (ii) Educational Qualification; (iii) Details of spouse; (iv) Details regarding children; (v) Other Information which can include queries on a) Car/two-wheeler ownership, b) has a credit card c) has an insurance Policy.

The Company shall, where its Customer submits a proof of possession of Aadhaar Card containing Aadhaar Number, ensure redacts or blacks out of his Aadhaar number is done through appropriate means.

12.CUSTOMER EDUCATION

The Company will take adequate measures to educate the Customers on the objectives of the KYC programme, especially at the time of obtaining sensitive or personal information from the Customers. When required to collect any information about the Customer for the purpose other than KYC requirement, it will not form part of the loan application. Such information

will be collected separately, purely on a voluntary basis in a form prescribed by the Company after explaining the objective to the Customer and taking the Customer's express approval for the specific uses to which such information could be used. The customer servicing staff is specially trained to handle such situations while dealing with Customers. The Company takes care to see that implementation of the KYC guidelines in respect of customer acceptance, identification etc. do not result in denial of opening of new loan.

13. CUSTOMER DUE DILIGENCE PROCEDURES ("CDD")

The Company shall perform CDD procedures for accepting account based relationship with customers, identification of beneficial owners, ongoing due diligence and periodic updation of KYC records.

In addition to above, the Company shall undertake enhance due diligence for onboarding non-face to face customers and politically exposed person.

Adequate CDD procedures would be deployed by the Company in respect of accounts opened by professional intermediaries on behalf of clients.

Ongoing Due Diligence

Ongoing monitoring is an essential element of effective KYC procedures. The Company effectively controls and reduces the risk through understanding of the normal and reasonable activity of the Customer and by it having the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The Company should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts will be subjected to intensify monitoring.

Illustrative list of activities which is construed as suspicious transactions

- Activities not consistent with the Customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- Any attempt to avoid reporting/record-keeping requirements/provide insufficient/ suspicious information:
- A Customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
- Certain employees of the Company arousing suspicion:
- An employee whose lifestyle is beyond his/her economic means
- Negligence of employees/willful blindness is reported repeatedly.

- Multiple accounts under the same name.
- Refusal to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.
- There are reasonable doubts over the real beneficiary of the loan. Frequent requests for change of address.

The company may adopt appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

Review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months. The Company shall also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation shall not be less than once in ten years in case of low risk category customers, not be less than once in five years in case of medium risk category customers and not less than once in two years in case of high risk categories in the following manner. The Company shall ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk.

Notwithstanding the provisions given above, in respect of an individual customer who is categorized as low risk, the Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC. The Company shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

1. INDIVIDUAL CUSTOMERS	
a) No change in KYC information	A self declaration from the customer in this regard to be obtained through customer's email-ID, customer's mobile number registered with us, Mobile application, Letter etc.
b) Change in address	A copy of OVD or deemed OVD or equivalent e-documents as per KYC Policy for the new address to be obtained from the customer through customer's email-ID, customer's mobile number registered with us, Mobile application and Letter etc.
c) Accounts of customers who were minor at the time of opening account on their becoming major	A fresh photograph shall be obtained from the customer on their becoming a major and it shall be ensured that CDD documents as

	per the current CDD standards are available with the Company. The Company may also carry out fresh KYC of such customers, wherever required.
d) Accounts opened using Aadhaar OTP based e-KYC, in non- face-to-face mode	Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud. The specific conditions stipulated for opening of an account using Aadhar OTP in non-face-to-face mode under RBI guidelines are not applicable for updation/ periodic updation of KYC.
2. CUSTOMERS OTHER THAN INDIVIDUALS (LEGAL ENTITY)	
a) No change in KYC information	In case of no change in the KYC information of the LE customer, a self-declaration to be obtained from the LE customer through its email ID registered, mobile application, letter from an official authorized by the LE in this regard, board resolution etc. Beneficial Ownership (BO) information available to be reviewed and updated.
b) Change in KYC information	To undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.
3. ADDITIONAL MEASURES	
a) The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.	
b) Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.	
c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self- declaration from the customer, for carrying out	

periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.	
d) In order to ensure customer convenience, Company may consider making available the facility of periodic updation of KYC through online portal as well as at branch level.	
e) The Company shall adopt a risk based approach with respect to periodic updation of KYC.	
4. OBLIGATIONS OF CUSTOMERS	
Due Notices for Periodic Updation of KYC	The Customers are required to submit the updated KYC documents to the Company, in case of any updation in the KYC already submitted by the customer at the time of establishment of business relationship / account- based relationship and thereafter, as necessary, within a period of 30 days from such update in order to comply with the PML Rules.
	The Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of

	such advance intimation/ reminder shall be duly recorded in the Company's system against each customer for audit trail.

Enhanced Due Diligence

Enhanced Due Diligence will involve closely monitoring the account, frequently updating KYC documents, field investigation or visiting the customer, etc., which forms part of the credit policies of the businesses.

If the Company has Customers or accounts that are determined to pose a potential high risk including but not limited to non-face to face customers and thereby warrant enhanced scrutiny then it shall conduct Enhanced Due Diligence in connection with such Customers. The Company has established appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence. Enhanced Due Diligence shall be coordinated and performed by the Company as per the procedures stipulated by Reserve Bank of India in Master Direction (KYC), 2016 (DBR.AM.BC.81/14.01.001/2015-16 dated 25.02.2016) as amended from time to time.

The following are the indicative list where the risk perception of a Customer which is considered higher:

- Customers requesting for frequent change of address/contact details;
- Sudden change in the loan account activity of the customers; or
- Frequent closure and opening of loan accounts by the customers.

In case of sale of repossessed vehicles by company to purchasers/brokers, company shall ensure to collect the KYC (Identity & address proof) so as to ensure the real identity of the buyer of such repossessed vehicles. Company shall obtain a declaration from the buyer that vehicles are being sold by the Company on 'As is Where Is' basis and the buyer is responsible to ensure the name transfer in RTO Records and deletion of the Company's hypothecation thereon. This ensures Company / its original customers is not accountable for repossessed vehicles being used for terrorist or any other unlawful activities.

The Company obtains End Use Declaration letter from customers confirming the purpose of finance taken and a declaration that the Facility shall not be used for any illegal and /or anti-social and / or speculative purposes including but not limited to participation in stock markets / IPOs.

14. RISK RECORD MANAGEMENT ("RRM") AND MONITORING OF TRANSACTIONS:

1) The Board of Directors ("Board") of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles and principles for risk categorization of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

2) The Company shall abide by the provisions of Rules made in this behalf by the competent authorities.

3) In accordance with section 12 of the Act, the Company shall maintain and preserve the records pertaining to the customer due diligence and transaction monitoring upto the time limit of five (5) years as prescribed in that section.

4) The Company shall deploy physical as well as electronic systems for maintenance of 16 proper records in relation to transactions reportable in Rule 3 of the Rules. The information contain in the records shall be sufficient to permit reconstruction of individual transactions comprising:

a. Nature of the transactions;
b. The amount of transaction and currency in which it was denominated;
c. Date on which the transaction was conducted;
d. Parties to the transactions.

5) The Company shall evolve a system for proper maintenance and preservation of customer and account related information in a manner that allows easy retrieval as and when requested by the competent authorities.

6) While obtaining and preserving the customer records, the Company shall abide by the provisions of Digital Personal Data Protection Act, 2023 and the Rules made there under.

7) The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers.

15. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise regularly to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk.

b. The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.

c. The risk assessment by the Company shall be properly documented and be commensurate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

d. The outcome of the exercise shall be put up to the Risk Management Committee/Board on a annual basis and will be available to competent authorities and self-regulating bodies. The Company shall apply a Risk Based Approach ("RBA") for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

16. IDENTIFICATION

All customers shall be identified by a unique identification code. This unique code will be employed to track the facilities availed, monitor financial transactions which assists in risk profiling of customers. The customer identification requirement applicable to borrowers / investors and depositors are detailed in Annexure II to this Policy.

17. VERIFICATION

As a part of the Lending Policy, the Company documents and implemented appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the identity of its Customers (Borrower's). Verification of customer identity should occur before transacting with the Customer. The Company describes the acceptable methods of verification of customer identity, which includes verification through documents, non-documentary verification methods or additional verification procedures that are appropriate with the associated risks, which are explained below;

I. Verification through documents:

These documents may include but are not limited to the list of documents that can be accepted as proof of identity and address from customers by the Company as provided in the Lending Policy. The customer identification requirement applicable to borrowers / investors and depositors are detailed in **Annexure II** to this Policy.

II. Verification through non-documentary methods:

The Company depends on other methods of verification as listed below:
1. Contacting or visiting a Customer;
2. Independently verifying the Customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; or
3. Checking references with other financial institutions.

III. Additional verification procedures.

The Business Head advises the credit team to make a personal visit to address under the following situations.
1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The sales executive is not familiar with the documents presented;
3. Where the sales executive is otherwise presented with circumstances that increase the risk that it will be unable to verify the identity of a Customer through documents; and
4. If the sales executive cannot verify the identity of a Customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, to verify the customer's identity.

18. MAINTENANCE OF RECORDS OF TRANSACTIONS & IDENTITY

The Company has a system of maintaining proper record of transactions prescribed under Rule 3, of the PML Rules 2005 and value of transactions, the procedure and manner of maintaining and verification and maintenance of records of the identity of the clients as mentioned below:

- All cash transactions of the value of more than Rupees Ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below Rupees Ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten lakhs;

- All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- As per the RBI guidelines, the Company maintains the following information in respect of transactions referred to in Rule 3 of the Rules:
- Nature of the transactions;
- Amount of the transaction and the mode adopted for undertaking the transaction;
- Date on which the transaction was conducted; and
- Parties to the transaction.

19. PRESERVATION OF RECORDS

The Company will maintain the records containing information of all transactions including the records of transactions detailed in PML Rule 3. The Company should also take appropriate steps to evolve a system including establishment of appropriate AML / CFT Cell at HO Level for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

The Company should maintain records relating to the transactions, whether attempted or executed, in such manner & for such period as specified under section 12 of the Act.

The Company should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules. The identification records and transaction data including attempted & executed should be made available to the competent authorities upon request.

20. ACCOUNTS OF NON-FACE-TO-FACE CUSTOMERS

In the case of non-face-to-face customers, it should be ensured that the first payment is effected through the customer's KYC-complied account with another regulated entity.

21. CENTRAL KYC REGISTRY ("CKYCR")

a. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26,

2015.The Company will ensure that the Customer KYC information is shared with the CKYCR in the manner mentioned in the RBI KYC Guidelines as per the KYC templates prepared for 'Individuals' and 'Legal Entities'.

b. Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual/LE as the case may be.

c. Also, whenever the Company obtains additional or updated information from any customer with respect to his KYC, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Company regarding an update in the KYC record of an existing customer,the Company shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Company.

d. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

e. Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

    i) there is a change in the information of the customer as existing in the records of CKYCR;

    ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms;

    iii) the validity period of downloaded documents has lapsed;

    iv) The considers it necessary in order to verify the identity or address of the customer (including current address), or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

22.ACCOUNTS OF POLITICALLY EXPOSED PERSONS (PEPS)

A. The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

1. The Company have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
2. Reasonable measures are taken by the Company for establishing the source of funds / wealth;
3. The approval to open an account for a PEP shall be obtained from the Senior Management;
4. All such accounts are subjected to enhanced monitoring on an on-going basis;
5. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Senior Management's approval is obtained to continue the business relationship;

B. These instructions shall also be applicable to family members or close associates of PEPs.

Explanation: For the purpose of this section, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

23. APPOINTMENT OF DESIGNATED DIRECTOR

The Managing Director/Any Director of the Company shall be appointed as Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and Rules.

The Company shall submit the name, designation, address and contact details of the Designated Director to the FIU-IND and Reserve Bank of India (RBI), whenever there is any change.

24. APPOINTMENT OF PRINCIPAL OFFICER

The Chief Executive Officer shall be appointed as Principal Officer of the Company, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under PML Act/ KYC Policy.

The Company shall submit the name, designation, address and contact details of the Principal Officer to the FIU-IND and Reserve Bank of India (RBI), whenever there is any change.

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

25. REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA (FIU-IND)

The Company is registered with FIU-IND with registration number of _____.

The Company shall furnish the following reports to the Financial Intelligence Unit-India (FIU- IND), with regard to information referred to in Rule 3 of the Rules and in terms of Rule 7 thereof in the manner so specified and within the timelines prescribed therein;

a. Cash Transactions Report **("CTR")**
b. Suspicious Transactions Report **("STR")**
c. Counterfeit Currency Reports **("CCR")**
d. Non-Profit Organization Reports **("NPR")**

The Company has implemented a system not to accept cash of more than Rs. 2 lakhs at a time from its borrowers. Hence, it normally does not and would not have large cash transactions. However, when cash transactions monthly aggregating of more than Rs. 10 lakhs are undertaken, the Company will maintain record of all such cash transactions in a separate register at its corporate office.

The Company monitors transactions of a suspicious nature on an ongoing basis for the purpose of reporting it to the appropriate authorities. The extent of monitoring by the Company depends on the risk sensitivity of the account and special attention is given to all complex unusually large transactions, which have no apparent economic or lawful purpose. The Company shall promptly report such high value cash transactions or transactions of a suspicious nature to the appropriate regulatory and investigating authorities. The Company has a system which alerts inconsistent transactions and profile of the customers is updated for effective identification and reports of suspicious transactions.

26.CONFIDENTIALITY OF INFORMATION

Information collected from Customers for the purpose of opening of account shall be treated as confidential and in accordance with the agreement/terms and conditions signed by the Customers. The information collected from Customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the Customer. While considering the requests for data/information from Government and other agencies, the Company shall satisfy that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in their transactions.

The exceptions to the said rule shall be as under:

a. Where disclosure is required under law;
b. Where there is a duty under the law to disclose such information;
c. Where the disclosure is made with the express or implied consent of the Customer subject to the provision of Digital Personal Data Protection Act, 2023.

27. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

The Company must have an ongoing employee training program on at least half yearly basis so that the members of the staff are adequately trained in KYC procedures. Training requirements have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

There should be open communication, high-integrity, proper understanding of subject matter amongst the Company's staff dealing with KYC/AML matters.

28. INVESTOR KYC POLICY

The Company's guidelines pertaining to four Key elements viz. Customer Acceptance Policy, Risk Management, Customer Identification Procedures, Customer Due Diligence and Risk Record Management & Monitoring of Transactions of this KYC framework, mentioned in this Policy will be equally applicable for its investors with suitable modifications depending upon the activity undertaken. The Company shall ensure that a proper framework on KYC and antimoney laundering standards are put in place in this regard. Basic KYC shall be completed through details like Certificate of Incorporation, PAN, TIN, GST etc. All funding proposals will be subject to proper checks on OFAC/ FATF / UN Sanctions List circulated by RBI / List of Willful defaulters / Other List of Terrorist Organizations.

The FATF periodically identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in its following publications:
a) High-Risk Jurisdictions subject to a Call for Action, and
b) Jurisdictions under Increased Monitoring.

In compliance of RBI's Circular regarding Investment in NBFCs from FATF non-compliant jurisdictions dated February 12, 2021, the Company promotes investments from FATF compliant jurisdiction, i.e. from entities whose name does not appear in the aforementioned lists. Records of such checks shall be maintained.

29. REVIEW OF POLICY/AMENDMENT

The Board of Directors reserves its right to review and amend this policy to ascertain its appropriateness as per the needs of the company. Review shall be carried out at least once a year. In the event of any conflict between the provisions of this Policy and the RBI or any other statutory enactments, rules, the provisions of such RBI or statutory enactments, rules shall prevail over this Policy. The Board may, subject to applicable laws amend any provision(s) or substitute any of the provision(s) with the new provision(s) or replace the Policy entirely with a new Policy.

Annexure I

Indicative list for Risk Categorization:

Sr. No.	Low Risk (Level 1)	Low Risk (Level 1)	High Risk (Level 3)
1	Students, Housewives, Pensioners.	Non-Banking Financial Institutions.	Politically Exposed Persons & their relatives.
2	Salaried Persons	Credit Co-Operative Societies	Politically Exposed Persons & their relatives.
3	Shareholders of the company	Non-Scheduled UCBs	Accounts of construction & real estate dealers & brokers
4	Small Traders	Travel Agents	Trusts / NGOs / Organizations receiving donations
5	Self-Employed	Dealers in Pharmaceuticals	Persons with dubious reputation, knowledge of which is available in public domain
6	Self Help Groups	Dealers of Wholesale electronic materials	Accounts, being subject to investigation by law enforcement agencies.
7	Staff & their relative accounts	Advocates, Solicitors & Notaries	Names 100% matching with the Persons notified by UNSC.
8	Co-Operative Housing Societies	Dealers in new as well as used two wheelers	Persons with criminal background, knowledge of which is available in public domain.
9	Professionals such as CA, CS, CMA, Doctors, Engineers, Consultants	Used car sellers	Dealers in antiques
10	Agricultural & allied activities	Dot Com Companies or internet service providers	Dealers in arms
11		Auctioneers	Share brokers
12		Restaurants & Bar	Unclaimed deposit accounts
13		Telemarketers & Telecommunication service providers	Money Changes / Remitters
14		Internet Café	New opened accounts for first 6 months
15		IDD Call Service Providers	KYC Non-Compliant Accounts
16			Non Face to Face Customers Eg. POA Accounts. *Minor Accounts
17			Firms with sleeping partners
18			HNI Customers
19			Customers appearing to be Multi-Level Marketing Companies
20			Clients managed by professional service providers such as law firms, accountants, brokers, etc.

21			Customers with High Net Worth (above Rs.1 Crore)

*Minor Accounts = Risk Categorisation will be as per their Guardian Account (Guardian Profile).

Annexure II

Customer Identification Procedure – the documents that may be obtained from borrowers

Nature of customer	List of applicable documents
Individual	The Company shall obtain the following from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity: a) a certified copy of any OVD containing details of his identity and address; and b) the Permanent Account Number (PAN) or Form no.60; and c) One recent photograph d) Such other documents in respect of nature of business and financial status of the customer, or the equivalent e-documents thereof, as may be required by the by the Company from time to time. e) the KYC Identifier with an explicit consent to download records from CKYCR. <u>List of OVDs</u>: i) Passport, ii) Driving license iii) Proof of possession of Aadhaar number iv) Voter's identity card issued by the Election Commission of India v) Job card issued by NREGA duly signed by an officer of the State Govt. vi) Letter issued by the National Population Register containing details of name and address. Provided that: 1) Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the UIDAI. 2) Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:- i) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii) Property or Municipal tax receipt; iii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv) Letter of allotment of accommodation from employer issued by State Govt. or Central Govt. Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation. The Credit Head of The Company has the power to approve the following documents in lieu of ID and address proof. **In lieu of Identity proof** Notarized copy of Marriage certificate with the applicant photograph.

	Explanation: A document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name. **In lieu of address proof** • Rental agreement along with rent receipt and utility bill of the Landlord. • In case the customer has a temporary address being a transit arrangement provided by real estate builder – Allotment letter issued by the builder + permanent address proof • In deserving cases where there is no address proof for one of the applicants or guarantors, an affidavit signed by a close relative (only in case of spouse, parents or children) confirming that the co applicant / guarantor is staying together in the same address. 3. The Credit Head of The Company jointly with the concerned Sales Head has further delegated the approval powers to accept the above documents to credit managers, as they may deem fit and necessary, in this regard. 4. In the event of any genuine reason for non-availability of any of the prescribed documents or to approve any deviations for change in the documents prescribed under this Policy, the Credit Head jointly with the Sales Head considers approving any other document not stated above based on the product, market requirements and also on the merits of the case. **Identification number:** 1. A taxpayer identification number; passport number and country of issuance; letter issued by Unique Identification Authority of India containing AADHAAR number; or number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government issued documentation certifying the existence of the business or enterprise; 2. For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but business process has implemented procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period before disbursal of loan. The Company also ensures that all the customers namely applicant, co applicants and guarantor has valid ID proof as prescribed above 1. The Credit Head of The Company has the power to approve the following document in lieu of ID and address proof ✓ *A Certificate from the public authority (i.e) Gazette Officer of State or Central Govt. / Magistrate/ MRO/ VRO/ Gram Panchayat Sarpanch/ notary public.*
Companies	1. Certificate of Incorporation, Memorandum of Association and Articles of Association 2. Resolution of the Board of Directors to open an account and identification of those who have the authority to operate the account. 3. Power of Attorney granted to its managers, officers or employees to transact business on its behalf 4. PAN Allotment Letter 5. Telephone Bill

	6. GST number 7. Names of the relevant persons holding senior management position 8. The registered office and principal place of its business, if it is different
Partnership Firms/ LLPs	1. Registration Certificate if the partnership deed is registered 2. Address of the registered office and principal place of its business, ifit is different 3. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf 4. Any official valid documents identifying the partners and the persons holding the power of attorney and their addresses 5. Telephone bill in the name of firm/partners Accounts 6. PAN 7. GST number (if any)
Proprietary Concerns	1. Proof of the name, address and activity of the concern like registration certificate (in case of a registered concern) including Udyam Registration Certificate (URC) issued by Government. 2. Certificate issued by the Municipal authorities under the Shops and Establishment Act, GST returns, Income Tax returns, GST Certificate, Registration documents issued by GST, Professional Tax Authorities, Certificate of Practice issued by Food and Drug Control Authorities etc. 3. Any registration documents issued in the name of the proprietary concern by the central government, state government. We also accept IEC (import-export code issued to the proprietary concern by the office of DGFT as an identity document for opening of account. 4. Income Tax return copy in the name of the sole proprietor where the firm's income is reflected duly authenticated by the Income Tax Authorities 5. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern Any two of the above documents would suffice. These documents should be in the name of the proprietary concern
Trusts, foundation s and society	1. Names of trustees, settlers, beneficiaries and signatories. 2. Names and addresses of the founder, the managers/ directors and the beneficiaries. Telephone/fax numbers 3. Names of beneficial owners 4. Certificate of registration, if registered, Trust Deed, PAN or Form 60 of the Trust, Power of Attorney granted to transact business on its behalf. 5. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founder's/managers/ directors and their addresses. 6. Resolution of the managing body of the foundation/ association. 7. Telephone bill 8. the names of the beneficiaries, trustees, settlor and authors of the trust 9. the address of the registered office of the trust; and 10. list of trustees and documents, for those discharging role as trustee and authorized to transact on behalf of the trust 11. Satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

*****End of Policy Document*****