Know Your Customer Norms (KYC)
And Anti Money Laundering (AML) Measures

Namdev Finvest Limited
(Formerly Known as Namdev Finvest Private Limited)

Registered Office:
"Namdev House"
Plot No. 21, Neer Sagar-A, Bhankrota,
Jaipur, Rajasthan – 302026, India

CIN: U65921RJ1997PLC047090

Policy Name	**Know Your Customer Norms (KYC) And Anti Money Laundering (AML) Measures**	
Version	**3.0**	
Effective date of this version	**May 2026**	
Next review date	**FY 2027-28**	
Prepared and proposed by	**Ms. Sakshi Sharma**	
Approver	**Board of Directors**	**May 2026**

INDEX

1. Introduction

Namdev Finvest Limited (NFL) formerly known as **Namdev Finvest Private Limited** is a Non-Banking Financial Company having valid Certificate of Registration with Reserve Bank of India vide registration No. B-10.00260 on 20th August 1997 under current RBI classification as NBFC – Non-Deposit taking Investment and credit company ("NBFC-ICC") under NBFC Middle Layer – RBI (NBFC-Scale Based Regulation) Directions, 2023.

It is focused on offering finance to MSME, Two-wheelers, Solar panel loan, Electric Vehicle (EV) loan, EV charging station loan and all kind of light commercial vehicles segment.

2. Objectives

To lay down explicit criteria for acceptance of customers.

- To establish procedures to verify the bona-fide identification of individuals/ non individuals before becoming an account holder/customer.
- To enable the Company to know/understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.
- To comply with applicable laws and regulatory guidelines.
- To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.
- To prevent criminal elements from using the Company for money laundering activities.

3. Scope

This policy is applicable to all branches and all other offices of the Company.

4. Definitions

i. Customer

A "Customer" for the purpose of this policy is defined as:

- A person or an entity that maintains an account and/or has a Business relationship with the Company.
- One on whose behalf the account is maintained i.e. the Beneficial Owner.
- Beneficiaries of transactions conducted by Professional Intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law and
- Any person or entity connected with a financial transaction.

ii. Money laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the "offence of money laundering' as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds or crime and projecting it as untainted property shall be guilty of offence of money laundering".

iii. Customer Due diligence (CDD)- means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. The CDD shall be include identify and verification of the customers identity, information on the purpose and intended nature of the business relationship, where applicable, nature of the customer's business, ownership and control, identity of the beneficial owner of the customer.
Further the company may obtain KYC identifier with explicit customer consent to download KYC s from CKYCR for the purpose of CDD.

iv. Central KYC Records Registry (CKYCR)- means the company to ensure overall compliance with the obligation imposed under chapter IV of the PML act and rules.

v. Know Your Customer (KYC) Identifier – means the unique number or code assigned to a customer by the Central KYC records registry.

vi. Equivalent e-document – means as 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 Rules 2016.

vii. Official Valid Documents (OVD) – means the passport Driving license, Proof of possession of Aadhar Number, Voter's Identity card, 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/her proof of possession of Aadhaar number as an OVD, he/she 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: -

- utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- property or Municipal tax receipt;
- pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- 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 license 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) (as and when applicable) 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.

viii. "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.

ix. Senior Management – as defined in Nomination and Remuneration Policy of the company

x. Suspicious transaction – means a transaction including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence regardless of the value involved; or
- Appears to be made in circumstances of unusual or unjustified complexity; or
- Appears to not have economic rationale or bona fide purpose' or
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- Video based customer identification process (V-CIP) – means an alternate method of Customer Due Diligence carried out by the Company through a live, audio-visual interaction with the customer, in order to establish and verify the identity of the customer, in accordance with the guidelines issued by the Reserve Bank of India from time to time.
- The V-CIP process shall be treated as a face-to-face onboarding method and shall be conducted by an authorized official of the Company, subject to the requirements prescribed under master direction:

xi. Wire Transfer – for the purpose of this policy, wire transfer and its related definition would have the same meaning as assigned to it under the RBIs guidelines on "Know your Customer" and Anti Money Laundering measures as amended from time to time.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the RBI Guidelines and other regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

5. Money Laundering and Terrorist Financing Risk Assessment:

a) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering & terrorist financing risk and shall properly document the risk assessment.
b) Further, the periodicity of risk assessment exercise shall be annual.
c) The outcome of the exercise shall be put up with the Risk Management Committee.
The Company shall apply a Risk Based Approach (RBA) and implement a CDD programme, having regard to the ML/TF risks identified by the Company and the size of business for mitigation and

management of the identified risk and establish controls and procedures in this regard which shall be monitored regularly and enhance them if necessary.

6. Know Your Customer Standards

The revised KYC policy of the Company incorporates the following four elements:

- Customer Acceptance Policy (CAP)
- Customer Identification Procedures (CIP)
- Monitoring of Transactions; and
- Risk Management

a. Customer Acceptance Policy (CAP)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the Company. The branches shall accept customer strictly in accordance with the said policy:

- The Company will have an elaborate standard for obtaining comprehensive information regarding new customers at the initial stage and that of existing customers over a predetermined period, thereby establishing the Bonafede's of customers opening credit accounts with the Company.
- The Company will lay down/spell clearly the document requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the guidelines issued by Reserve Bank of India from time to time i.e. nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc.
- The Company shall assign a Unique Customer Identification Code (UCIC) to each customer at the time of onboarding, following the completion of Know Your Customer (KYC) procedures as prescribed by the Reserve Bank of India (RBI). This shall include verification of identity, address, and risk categorization based on prescribed parameters. The Company shall establish a robust mechanism to prevent the duplication of UCICs and shall ensure that the same UCIC is used across all products and services availed by the particular customer.
- Further, during the onboarding process of potential customers, their respective KYC details shall cross-verify automatically against the existing customer database. If a potential match is identified, the system flags the existing record under deduplication ("dedupe"). A new UCIC shall be generated only if no matching KYC details are found in the current database. Furthermore, the Company conducts periodic audits and system validations to further strengthen the effectiveness of the de-duplication mechanism.
- The Company will not open accounts in the name of anonymous/fictitious/ benami persons.
- The Company will ensure that circumstance in which a customer is permitted to act on behalf of another person/entity will be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in the fiduciary capacity.
- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;
- Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking as

there shall be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in the fiduciary capacity and

- The Company will ensure that before opening a credit account there are adequate checks to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities like individual terrorist or terrorist organizations.
- The Company shall consider filing a Suspicious Transaction Report (STR) if unable to comply with CDD measures due to non-cooperation or unreliable documents.
- No account will be opened if the customer's identity matches with names in RBI/FIU-IND sanctions lists.
- Whether Permanent Account Number (PAN) details obtained, shall be verified from search/verification facility of the issuing authority.
- Equivalent e-documents shall be verified for digital signature as per the provisions of Information technology Act, 2000
- Implementation of the KYC norms should not result in denial of services (including opening of credit account) to the public, especially to those, who are financially or socially disadvantagedincluding the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned. The low-income group both in urban and rural areas should not be denied services merely for the reason that they are unable to produce documents to satisfy the Company about their identity and address.
- Adoption of customer acceptance policy and its implementation shall not become too restrictive and the Company will strive not to inconvenience the general public, especially those who are financially or socially disadvantaged including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

b. Customer Identification Procedure (CIP)

Identification is an act of establishing who a person is. In the context of KYC, it means establishing who a person purports to be and will involve identifying the customer and verifying his/her identities by using reliable and independent source documents, data or information. For this purpose, the Company will obtain sufficient information necessary to establish to its satisfaction the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

The Company shall perform the Customer Due Diligence (CDD) either on its own or can rely on the CDD conducted by any third party, subject to obtaining the record or information from the third party or CKYCR on an immediate basis and being ultimately responsible for the identity of the Customer.

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.

Identity is verified for:

- The named account holder
- Beneficial owner's
- Signatories to an account and

- Intermediate parties.

i. Accounts of Individuals

In case of customers that are natural person the Company will obtain sufficient identification data to verify
(a) The identity of customer
(b) his/her address/ location and
(c) his/her recent photograph. The true identity and bonafide of the existing customers and new potential customers opening credit accounts with the Company and obtaining basic background information would be of paramount importance.

ii. Other than individual accounts

For customers that are legal person or entities the Company will

- Verify the legal status of the legal person/entity through proper and relevant documents,
- verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person,
- Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

iii. Accounts of companies and firms

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.

iv. Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The branches should seek prior approval of their concerned Credit Heads for opening an account in the name of PEP.

v. Accounts of proprietary concerns

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, the Company should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

Proof of the name, address and activity of the concern, like registration certificate including udyam registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns,

CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. the Company may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

7. Obtaining Guarantor on credit facilities

The Company generally insists on "Guarantee" by a known person (who becomes guarantor to a particular credit facility). Obtaining Guarantee from a known person is a process of ascertaining the identity of a person and his acceptability for establishing business relationship and verifying the true identity of the intending customer before opening a credit account. Further, Guarantor also acts as an introducer of the customer to the Company for the credit facilities.

8. Liabilities of the Guarantor

Guarantor is legally responsible to the Company for the repayment of the credit facilities by the customer and is expected to be in a position to identify/trace the account holder in case of need.

9. Procedure for providing Guarantee

The Guarantor will be required to sign on the agreement entered into with the Customer at various places provided in the loan agreement form.
The Guarantor will be normally required to visit the Company's branch for signing the agreement. However, this need not be compulsory.

10. Closure of accounts

Where the company is unable to apply appropriate KYC measures due to no furnishing of information and /or non-cooperation by the customer, the company will consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions will be taken at a reasonably senior level.

11. Monitoring of Transactions

- **Ongoing Due Diligence**

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.
The company may adopt appropriate innovations including intelligence and machine learning (AI & ML) to support effective monitoring.

The Company shall prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits, Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. Further, there are no operative accounts where in the need for fixing the threshold limits for individual transactions and aggregate is more relevant and necessary. All the company's loans are EMI based loans on all categories of borrowers. Hence the transactions with the company are purely shall be restricted to the EMI payable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI payable, the threshold for turnover shall be restricted to the aggregate EMIs payable year after year. No other transactions whatsoever in nature, other than repayment of loan along with interest and such charges as may be prescribed by the Company from time to time, shall be carried out by the customer with the Company
The permanent correct address shall mean the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the company for verification of the address of the customer. In case utility bill is not in the name of the customer but is close relative: wife, son, daughter and parents etc. who live with their husband, father/mother and son, the company shall obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) is a relative and is staying with him/her. The company shall use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, company shall keep in mind the spirit of instructions issue d by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.
The company shall put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation 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 updating of customer identification data (including photograph/s) after the account is opened. The periodicity of such updating shall not be less than once in five years in case of low-risk category customers and not less than once in two years in case of high and medium risk categories.

The Company shall, as a general principle, discourage acceptance of third-party payments (i.e., payments made by any person other than the borrower, co-borrower, or guarantor) towards loan repayment, prepayment, or foreclosure. However, in exceptional and bona fide cases, such payments may be accepted subject to prior verification. The Company shall mandatorily obtain a written authorization from the borrower, KYC documents of the third party, details establishing

the relationship between the borrower and the third party, and a declaration regarding the source of funds. All such transactions shall be subject to monitoring and appropriate approvals as per internal thresholds, and any unusual or suspicious patterns shall be reported in accordance with applicable AML regulations. The Company shall not accept third-party payments where the identity of the payer or source of funds cannot be satisfactorily established or where there is any suspicion of money laundering or fraudulent activity. Proper records of such transactions and supporting documents shall be maintained in line with regulatory requirements, and any deviation from this framework shall be treated as a breach of the AML/KYC Policy.

A. INDIVIDUAL CUSTOMERS • No Change in KYC information	A self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc.
• Change in Address	A self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc. The Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of updation/periodic updation.
B. CUSTOMERS OTHER THAN INDIVIDUALS (Legal Entity) • No Change in KYC information	A self-declaration shall be obtained from the Legal Entity (LE) customer through its email id registered with the Company, ATMs, digital channels (such as online banking/internet banking, mobile application of Company), letter from an official authorized by the LE in this regard, board resolution etc. The Company shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.
• Change in KYC information	

	The Company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.
C. 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 updation/periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation/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) The Company shall adopt a risk based approach with respect to periodic updation of KYC.
D. OBLIGATIONS OF CUSTOMERS	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.

12. Enhanced Due Diligence

The Company needs to apply enhanced due diligence measures in case of customers onboarding through non-face-to-face method. Presently, the Company onboard the customers through physical verification, and it shall comply with the respective provisions of RBI KYC & AML Master Direction as and when Company starts the procedure of onboarding the customers through non-face-to-face mode or V-CIP.

The periodicity of risk assessment exercises shall be on a **half yearly basis** or such other periodicity as may be decided by the Risk Management Committee of the Board, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

The outcome of the risk assessment exercise shall be placed before the Risk Management Committee of the Board or such other Committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies, if required.

13. Risk Management

The Board of Directors 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 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.

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. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

The Company shall prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the company. However, while preparing customer profile the company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk. Illustrative examples of low risk customers would be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher

than average risk to the company may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Company may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

The various information so collected from different category of customers for the purpose of risk categorisation and related to perceived risk shall be non-intrusive basis, notwithstanding the need for availability of minimum required information to meet the regulatory requirements.

Example of customers requiring Lower due diligence may include:

A. Salaried employees with well defined salary structures,
B. People working with government owned companies, regulators and statutory bodies etc,
C. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
D. People working with public sector units
E. People working with Public Limited Companies and Multinational Companies

Example of customers requiring Medium due diligence may include:

A. Salaries applicant with variable income/unstructured income or salary receiving in cash or cheque
B. Salaried applicant working with Private Limited companies related to travel agents, telemarketers, internet café, international direct dialling call service
C. Companies having close family shareholding or beneficial ownership

Examples of customers requiring higher due diligence may include: -

A. Non-resident customers,
B. High net worth individuals,
C. Trusts, charities, NGOs and organizations receiving donations,
D. Firms with 'sleeping partners',
E. Politically exposed persons (PEPs) of foreign origin,
F. Non-face to face customers, and
G. Those with dubious reputation as per public information available, etc.
H. Gambling/gaming including "junket operators" arranging gambling tours
I. Jewellers and Bullion dealers

Gradation of Risk can be defined by below mentioned table:-

Parameters	Low	Medium	High
FOIR	<50%	50% to 55%	>55%
LTV	<50%	50% to 55%	>55%
Customer Profile *	Good	Average	Poor
Age	22-50 Yrs	51-70 Yrs	18-21 Yrs & above 71 Yrs
Credit Bureau Score (Cibil)	>650	550 to 650 & NTC	<550

- For customer profile wise gradation of risk, refer annex A.

14. Combating Financing of Terrorism

In terms of PMLA Rules, suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. The company shall, before opening any new account, ensure that the name/s of the proposed customer does not appear (screening) in the list of RBI, World Bank, UN, EU and OFAC sanctions lists and International Finance Corporation exclusion list. Further, the company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to RBI and FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the company as an integral part of recruitment/hiring process of personnel.

15. Central KYC Records Registry (CKYCR) Compliance

The Company shall ensure compliance with the requirements of the Central KYC Records Registry (CKYCR) in accordance with the provisions of the Prevention of Money Laundering Act, 2002 and the applicable guidelines issued by the Reserve Bank of India from time to time.

In this regard, the following shall be adhered to:

- The Company shall upload the KYC records of all new customers, as well as updated KYC records of existing customers, to the Central KYC Records Registry within the prescribed timelines.
- The Company shall obtain and use the **KYC Identifier (KYC ID)** generated by CKYCR for the purpose of KYC verification. Where a customer submits a KYC Identifier, the Company shall retrieve the customer's KYC records from CKYCR and shall not insist on submission of the same KYC documents again, unless:
    - there is a change in the information of the customer;
    - the current address requires verification; or
    - the Company considers it necessary to verify or update the customer's details based on its risk assessment.
- The Company shall ensure that no duplication of KYC records takes place and shall rely on the KYC records available in CKYCR, subject to due verification.
- The Company shall take necessary steps to ensure that the KYC data uploaded to CKYCR is accurate, complete, and updated, and shall maintain confidentiality and security of such information at all times.
- The Company shall comply with all operational guidelines, standards, and procedures issued by CKYCR, RBI, or any other competent authority in this regard.

- The Company shall maintain transaction records 5 years from transaction date and KYC records- 5 years after relationship ends.
- No changes in KYCs are allowed without valid prior consent of concerned customers.

16. Wire Transfer

Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. The Company shall follow the responsibilities, procedure and other obligations applicable to the Company laid down in the rules for wire transfer occurring either domestic or cross- border of RBI KYC & AML Master Direction.

17. Cash and Suspicious Transaction Reports

A. Cash Transaction Report (CTR)

In terms of the Prevention of Money Laundering Act (PMLA), 2002, the company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND).

For determining integrally connected cash transactions, NBFCs shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds or equal to Rupees Ten lakh during the month.
CTR should contain only the transactions carried out by the company on behalf of their clients/customers excluding transactions between the internal accounts of the bank. A summary of cash transaction report for the bank as a whole should be compiled by the Principal Officer of the company every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

B. Suspicious Transaction Reports (STR)

The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer of the company shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from the company or any other branch office. Such report will be made available to the competent authorities on request.

Further the company shall not put any restrictions on operations in the accounts where an STR has been made. The company and its employees shall keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information.

(i) Maintenance of records of transactions

The company shall maintain the proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

- all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh 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 Lakh;
- all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency;
- 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 or a document has taken place facilitating the transaction and
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

(ii) Information to be preserved

The company will maintain all necessary information in respect of transactions referred to in Rule 3 to permit reconstruction of individual transaction, including the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

(iii) Maintenance and Preservation of Records

The company will maintain the records containing information of all transactions including the records of transactions detailed in Rule 3 above. The company should also take appropriate steps to evolve a system 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.

Further, in terms of PML Amendment Act 2012 notified on February 15, 2013, the company should maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

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 should be made available to the competent authorities upon request.

(iv) Reporting to Financial Intelligence Unit – India

In terms of the PMLA Rules, the company will report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India, 6th Floor,
Hotel Samrat, Chanakyapuri,
New Delhi -110021
Website - http://fiuindia.gov.in/

18. Education/Employee's Customer Training/Employee's Hiring

a) Customer Education

The Company recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose. Also provide declaration for compliance of Anti Money laundering.
Customer awarness sessions shall be conducted for spreading awarness.
The front desk staffs need to be specially trained to handle such situations while dealing with customers.

b) Employees' Training

The company must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. 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.

c) List Compilation

Employees must compile with list of UK and UN sanction list and any other list circulate by regulators.

d) Appointment of Principal Officer:

The Company shall designate any senior management or equivalent (know as Chief Executive officer, Chief Compliance Officer, Company Secretary, Chief Financial Officer, Chief Treasury Officer or any other equivalent) or any director as 'Principal Officer' (PO) who shall be located at the Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. However, in absence of Company Secretary, the Chief Financial Officer of the Company shall be considered as the principal officer

of the Company until a Company Secretary is appointed. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

e) Appointment of Designated Director:

The Board of Directors shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. The "Designated Director" can be a person who holds the position of senior management or equivalent. Accordingly, the Chief Executive Officer of the Company will be nominated as Designated Director by the Board of the Company. However, in absence of the Chief Executive Officer, the Managing Director of the Company shall be considered as the Designated Director of the Company until a Chief Executive Officer is appointed. It shall be ensured that the Principal Officer is not nominated as the "Designated Director". The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

19. Validity

The Policy shall be valid till review by committee members or Board of Directors of the company.

20. Review

The Company's CEO, CFO, CCO and COO have been entrusted with the responsibility of enforcement of this policy. They are hereby given absolute power to jointly or severely, make necessary changes, amendments or additions or removals for the operational aspects of the policy within the overall spirit and guidance from time to time for reasons like technology or process upgradation, regulatory changes, maintaining competitive edge or responding to changes in market or risk environment, etc. This is required to ensure full operational freedom to the senior management and make the management team more adaptive to rapid changing external environment. All changes so made shall be noted to the policy approving authority during the next policy review.

The CEO, CFO, CCO and COO can decide on delegation of authority and can design / redesign MIS systems and reporting as they see fit to improve the responsibility and accountability within the team hierarchy.

Annex A- Customer Profile wise Risk Gradation

EMP TYPE CATEGORY	Type of business	Profile
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PRIVATE LIMITED COMPANY (PVT. LTD. COMPANY)	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	LIMITED COMPANY (LTD. COMPANY)	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PROPRIETOR	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PARTNERSHIP FIRM	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	RETAIL SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MEDICAL SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	WHOLESALER	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SHOPKEEPER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	JUICE CENTRE	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CONTRACTOR	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FREELANCER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PLUMBER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	ELECTRICIAN	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CIVIL CONTRACTOR	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MASON (KARIGAR)	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	COMMISSION AGENT	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SKILLED CONTRACTOR	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	HARDWARE SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PLYWOOD SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	DRY CLEANER SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	RESTAURANT	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	HOTEL OR GUEST HOUSE	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CLOTH SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	JEWELLRY SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FURNITURE SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	AUTOMOBILE AND PARTS SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	AUTOMOBILE SHOWROOM	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	READYMADE GARMENT SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SHOE SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TAILOR SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	VEGETABLE AND FRUIT SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	VEGETABLE AND FRUIT CART	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	ELECTRONICS SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SANITARY ELECTRIC SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PETROL PUMP	Negative
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	DAILY WAGE LABORER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	AGRICULTURAL WORKER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	DRIVER	Good

SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TAXI OWNER/DRIVER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TRANSPORTATION WORK	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	HOSPITAL	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CLERICAL WORKERS	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SKILLED WORKERS	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CARPENTER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PAINTER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	WELDER	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MECHANIC	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FABRICATION SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FITNESS CENTRE	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FITNESS TRAINER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SECURITY PERSONNEL	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	BAKERY	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CATTLE BROKER	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	HAIR SALON	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	BEAUTY PARLOUR SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SWEET/MISTHAN BHANDAR	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	BUILDING MATERIAL SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TEA SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PAN SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	VEHICLE SERVICE CENTER	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	NEWS PAPAR HAWKER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	STATIONARY AND BOOK SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FAST FOOD SHOP / CART	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	BANGLES SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FLOWER SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	GIFT SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TENT HOUSE	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	BARTAN AND CROCERY SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MARRIAGE GARDEN	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FANCY STORE	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MEAT SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	BATTERY SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	OPTICAL SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	DJ SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MOBILE SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	DAIRY BOOTH	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	ICE CREAM PARLOUR	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	ICE CREAM CART	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	FLOUR AND MASALA MILL	Good

SELF-EMPLOYEED NON PROFESSIONAL (SENP)	MATTRESS SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TYRE SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CYCLE SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	CYCLE REPAIRING CENTER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SCRAP BROKER	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PRINTING SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	E-MITRA VENDOR	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PHOTOSTATE SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	PHOTOGRAPHER SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SPORTS ITEM SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	EGG CENTER	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	NAMKEEN BHANDAR	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	TYRE PUNTCURE AND REPAIRING SHOP	Good
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	AUTO PARTS SHOP	Poor
SELF-EMPLOYEED NON PROFESSIONAL (SENP)	SAREE SHOP	Good
AGRICULTURAL SECTOR	FARMER	Good
AGRICULTURAL SECTOR	DAIRY FARMER	Good
AGRICULTURAL SECTOR	HORTICULTURE	Good
AGRICULTURAL SECTOR	HYBRID AGRICULTURE	Good
AGRICULTURAL SECTOR	CATTLE FEED	Poor
AGRICULTURAL SECTOR	POULTRY FARM	Poor
SELF EMPLOYEED PROFESSIONALS (SEP)	DOCTOR	Good
SELF EMPLOYEED PROFESSIONALS (SEP)	LAWYER	Poor
SELF EMPLOYEED PROFESSIONALS (SEP)	CHARTERED ACCOUNTANT	Good
SELF EMPLOYEED PROFESSIONALS (SEP)	ENGINEER	Good
SELF EMPLOYEED PROFESSIONALS (SEP)	ARCHITECT	Good
SELF EMPLOYEED PROFESSIONALS (SEP)	IT PROFESSIONAL	Good
SALARIED	LIMITED COMPANY	Good
SALARIED	PRIVATE LIMITED COMPANY	Good
SALARIED	SEMI-GOVERNMENT	Good
SALARIED	PROPRIETORSHIP FIRM	Good
SALARIED	PARTNERSHIP FIRM	Good
SALARIED	NON-GOVERNMENTAL ORGANIZATION (NGO)	Good
SALARIED	TRUST	Good
SALARIED	STATE GOVERNMENT	Good
SALARIED	CENTRAL GOVERNMENT	Good
CASH SALARIED	PROPRIETORSHIP FIRM	Good
CASH SALARIED	PARTNERSHIP FIRM	Good
CASH SALARIED	NON-GOVERNMENTAL ORGANIZATION (NGO)	Good
CASH SALARIED	TRUST	Good