Nestavia Home Finance Private Limited

Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy

Name of the Policy: Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy

Policy Number: KYC-02/2025

PREAMBLE

Nestavia Home Finance Private Limited (hereinafter referred to as "the Company" or "Nestavia") is committed to providing the best possible customer experience through the customer first approach.

The Company recognizes its responsibility to promote good and fair practices by setting minimum standards in dealing with customers and thus has implemented this Know Your Customer (KYC) to establish clear guidelines and processes to establish the identity and address of the Customer and to prevent Nestavia Home Finance (Nestavia) from being used, intentionally or unintentionally, by criminal elements for money laundering activities. This policy is to enable Nestavia to understand the customers and their financial dealings better which in turn help to manage the risks prudently.

This Policy is framed in compliance with Master Direction – Non-Banking Financial Company – Housing Finance Company (Reserve Bank) Directions, 2021 **("RBI Master Directions")** (as amended from time to time) and all other applicable regulations.

Prepared and Proposed By	Compliance Officer
Reviewed and Recommended By	Managing Director & CEO
Approved By	Board of Directors
Date of Approval	07-Jul-2025

RESPONSIBILITY ASSIGNMENT MATRIX

Responsibility for Implementation	Branch Manager at each location and Compliance Officer at Corporate Office

VERSION CONTROL

Version No.	Date of Approval by Board of Directors	Key Highlights/Changes
1.0	23-Apr-2025	Roll-out of policy
2.0	07-Jul-2025	Inclusion of AML measures

Table of Contents

1. Objectives

This policy is designed to develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers and to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing. The objective is to:

- Establish identity and address of customers
- Understand the nature of the customer's activities
- Monitor transactions for suspicious activity
- Ensure compliance with RBI and PMLA guidelines

2. Regulatory Framework

This policy is framed under the following key regulations:

- RBI Master Direction – Know Your Customer (KYC) dated Feb 25, 2016 (updated periodically)
- Prevention of Money Laundering Act (PMLA), 2002 and rules thereunder
- RBI Master Direction – HFCs, 2021
- Guidance from Financial Intelligence Unit – India (FIU-IND)
- FATF Recommendations

3. Scope

This policy applies to:

- All individual and non-individual customers of the Company
- All products and services offered by the Company (home loans, mortgage loans, construction finance, etc.)
- All employees, authorized representatives and outsourced vendors involved in customer onboarding
- All branches of the Company

4. Definitions

- **Customer**: A person/entity maintaining a business relationship or carrying out a financial transaction with the Company.
- **KYC**: Process of verifying identity and address using OVDs (Officially Valid Documents).
- **CDD**: Customer Due Diligence under PMLA Rules.
- **FIU-IND**: Financial Intelligence Unit – India.
- **PEP**: Politically Exposed Person.
- **STR**: Suspicious Transaction Report.

---

5. Customer Acceptance Policy (CAP)

The Company shall:

- Accept only those customers whose identity and address can be verified using reliable documents.
- Not open accounts in fictitious/benami names.
- Not accept walk-in customers without proper due diligence.
- Define circumstances under which a customer may be refused onboarding (e.g., blacklisted entities, PEPs with adverse media). Politically Exposed Persons (PEPs), both domestic and foreign, shall be treated as high-risk customers irrespective of adverse media.
- Obtain **PAN** and Aadhaar as per regulatory guidance.
- Customers whose onboarding is declined due to KYC/AML concerns shall be informed of the reason and may seek redressal through the grievance redressal mechanism.

---

6. Customer Identification Procedure (CIP)

The Company shall identify the customer using:

a) For Individuals:

- Aadhaar (voluntary) / Voter ID / Passport / Driving Licence / NREGA Job Card (with photo)
- PAN (mandatory under PMLA)
- Recent photograph

- Proof of address (if not part of OVD)

b) For Non-individuals:

- Certificate of Incorporation
- PAN and GST
- Board Resolution
- Authorized signatories' OVDs and photographs
- Beneficial Ownership declaration as per Rule 9(3) of PMLA Rules

CIP will be applied at:

- Onboarding
- At the time of high-value transactions
- Periodically (for risk-based updates)
- Video-based Customer Identification Process (V-CIP) shall be used where applicable, as per RBI guidelines.
- CKYC compliance shall be ensured by uploading data to CKYCR within 10 days of onboarding and checking for existing CKYC numbers.

---

7. Risk Categorisation of Customers

Customers shall be categorized as:

Category	Examples	KYC Frequency
Low Risk	Salaried individuals, government employees, employees of public sector enterprises, senior citizens etc.	Every 10 years
Medium Risk	SMEs, professionals, unregistered bodies etc.	Every 8 years
High Risk	PEPs, NRIs, trusts, NGOs, charities, cash-intensive businesses etc.	Every 2 years

Criteria for risk categorization include:

- Nature of business
- Source of funds

- Geographical location
- Reputation

---

8. Ongoing Due Diligence

The Company shall:

- Monitor financial transactions to ensure consistency with customer profile.
- Conduct periodic KYC updates based on risk category.
- Re-verify identity if there's a change in ownership or profile.
- Trigger alerts for unusual or high-risk transactions.

---

9. Enhanced Due Diligence (EDD)

Applicable for:

- High-risk customers
- Customers from high-risk jurisdictions (FATF list)

Measures include:

- Additional documentation and verification
- Source of wealth verification
- Senior management approval before onboarding

---

10. Records Management

Records to be maintained:

- KYC documents: Minimum 5 years after account closure
- Transaction records: Minimum 5 years from date of transaction
- STR filings and logs: Indefinitely until permitted for destruction under applicable law or as directed by FIU-IND.

---

11. Reporting to FIU-IND

The Company shall:

- File Cash Transaction Reports (CTRs) for transactions > ₹10 lakhs.
- File Suspicious Transaction Reports (STRs) within 7 days of identifying suspicion.
- Nominate a Principal Officer (PO) and a Designated Director for compliance.

---

12. Monitoring of Transactions

Automated transaction monitoring shall be done to:

- Identify suspicious behaviour
- Generate alerts based on thresholds (e.g. cash deposits, multiple loan applications etc.)
- Support STR filings

---

13. Customer Education and Employee Training and Awareness

The Company shall:

- Train employees who interact with Customers to educate them when seeking KYC information
- Conduct annual KYC/AML training for all frontline and compliance staff.
- Provide updated regulatory guidelines and risk trends.
- Test awareness periodically.

---

14. Designated Director

The Designated Director shall oversee the compliance position of AML norms in the Company and the following will be adhered to in this regard.

a) A "Designated Director" means a person designated by Nestavia to ensure overall compliance with the obligations imposed under Chapter IV of the Act and shall be nominated by the Board of Nestavia;

b) The name, designation and address of the Designated Director including changes from time to time, shall be communicated to the Director, FIU-IND and also to the National Housing Bank; and

c) In no case, the "Principal Officer" shall be nominated as the "Designated Director")

---

15. Principal Officer

Principal Officer shall be located at the corporate office of Nestavia and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law and the following will be adhered to in this regard.

a) The name of the Principal Officer so designated, his designation and address including changes from time to time, may please be advised to the Director, FIU-IND.

b) Principal Officer will maintain close liaison with enforcement agencies, other HFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

c) Role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time.

d) The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than the applicable threshold in foreign currency to FIU-IND.

e) With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to customer identification data and other ODD information, transaction records and other relevant information

---

16. Policy review and amendments

This policy will be reviewed periodically by the Compliance department to ensure compliance with the law, reflect changes in business or regulatory requirements, and enhance its effectiveness. Any amendments will be communicated to customers and training provided to the employees.

---

17. Annexures

- **Annexure I**: List of Officially Valid Documents (OVDs)
- **Annexure II**: Customer Risk Categorization Matrix
- **Annexure III**: KYC Checklist – Individual and Non-Individual

---

Annexure - 1

List of Officially Valid Documents (OVDs)

For Individuals:

1. Passport
2. Driving Licence
3. Voter's Identity Card issued by the Election Commission of India
4. PAN Card
5. Aadhaar Card (voluntarily submitted and verified through UIDAI authentication, as per Aadhaar Act and RBI guidelines)
6. NREGA Job Card – duly signed by an officer of the State Government
7. Letter issued by the National Population Register containing details of name and address

Note:

- A valid Driving Licence or Passport is one that is not expired.
- Aadhaar can be accepted only if voluntarily submitted by the customer and must be verified via e-KYC or offline verification through UIDAI as permitted.

Proof of Address:

If the OVD submitted by the customer does not contain current address, then the following can be accepted as 'Deemed OVD' for address verification purposes only:

- Utility bill (electricity, water, telephone, gas) – not more than 2 months old
- Property or municipal tax receipt
- Pension or family pension payment orders
- Letter of allotment of accommodation from employer (for government employees)

These are acceptable only for address verification, not for identity.

For Non-Individual Customers:

Entity Type	**Required OVDs**
Company	- Certificate of Incorporation - PAN Card

Entity Type	Required OVDs
	- Board Resolution - Identification of Authorized Signatories (OVDs of individuals)
Partnership Firm	- Partnership Deed - PAN Card - Registration Certificate (if registered) - OVDs of partners and signatories
Trust	- Registration Certificate - Trust Deed - OVDs of Trustees
Sole Proprietorship	- Business registration certificate - GST/Tax filings - OVD of the proprietor
Unincorporated Association / Body of Individuals	- Resolution of the managing body - Power of attorney/authorization - OVDs of individuals managing the entity

KYC Verification Process Notes:

- All OVDs must be verified via:
    - Original sighting (for offline onboarding)
    - CKYC number (if available)
    - Digital KYC (e-KYC/Aadhaar offline, video KYC)
- Self-attested copies must be retained where applicable.
- Aadhaar usage must comply with Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Annexure -2

Annexure – Customer Risk Categorization Matrix

(To be read with Section 7 of the KYC/AML Policy)

Risk Parameter	Low Risk	Medium Risk	High Risk
Customer Type	Salaried individuals, government employees, employees of PSUs	Self-employed professionals, MSMEs	Trusts, NGOs, Charitable orgs, Shell companies
Nature of Business / Occupation	Government, PSU, MNCs	Retailers, Contractors, Service Providers	Arms dealers, casinos, real estate brokers, cash-intensive businesses
Geographical Location (residence or business)	Tier 1 to Tier 4 locations, low-risk FATF countries	Tier 5 to Tier 6 locations	High-risk jurisdictions, areas with known crime/terror activity
Source of Funds / Income	Salary in bank, verifiable through official documents	Income from business or rentals with moderate cash transactions	Unverifiable income, heavy cash dealings, foreign remittances with no clear source
Account Activity Profile	Predictable and consistent with known income	Irregular credits/debits, occasional large transactions	Frequent high-value transactions, unexplained credits or third-party transfers
Customer Profile Verification	Verified through official channels, documents in order	Minor discrepancies, require follow-up or clarification	Mismatch in documents, adverse media, negative background check
Politically Exposed Person (PEP)	Not applicable	Family member or close associate of PEP	Foreign PEPs or high-profile domestic PEPs
Type of Product / Loan Applied	Home loan for self-occupied residential unit	LAP (Loan Against Property), resale transactions	Loans involving third-party POA, layered ownership, high-risk projects
Delivery Channel	In-person onboarding through branch or approved agents	Digital onboarding with full KYC	Remote onboarding with limited physical

Risk Parameter	Low Risk	Medium Risk	High Risk
			verification, third-party sourced customers

Risk Categorisation Outcome:

Risk Score / Profile	Risk Category	KYC Update Frequency
Meets most Low Risk criteria	Low	Once every 10 years
Mix of Low & High or some Medium	Medium	Once every 8 years
Meets multiple High-Risk factors	High	Once every 2 years

Risk category must be reviewed at onboarding and during periodic KYC updates or on the occurrence of trigger events (e.g., change in ownership, suspicious activity, downgrade by risk engine etc.).

Note:

- Final risk classification should be validated by the Compliance Officer or Risk Team.
- Risk categorization should be documented in the Customer Onboarding Form or CRM.
- System-based alerts and flags should be configured to monitor high-risk accounts.
