

KYC-AML POLICY FOR AVA FINANCE PRIVATE LIMITED

1. INTRODUCTION:

AVA Finance Private Limited ("**Company**"), being a Base Layer Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India ("**RBI**"), is engaged in the business of providing consumer credit facilities, including payday loans, short-term personal loans and EMI-based loans to eligible borrowers.

The Company recognizes its responsibility to prevent its products, services and delivery channels from being used, intentionally or unintentionally, for money laundering, terrorist financing or any other unlawful activity.

Accordingly, the Company has adopted this Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) Policy ("**Policy**") to establish a robust framework for customer identification, customer due diligence, risk assessment, transaction monitoring, reporting and record maintenance.

This Policy has been formulated in accordance with:

- The Prevention of Money Laundering Act, 2002 ("**PMLA**") and rules framed thereunder;
- The Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time;
- Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016, as amended from time to time;
- Guidelines and instructions issued by the Financial Intelligence Unit – India (FIU-IND);
- Central KYC Records Registry (CKYCR) framework; and
- Recommendations and guidance issued by the Financial Action Task Force (FATF).

This Policy lays down the principles, systems, procedures and internal controls to ensure effective implementation of KYC, AML and CFT requirements across the operations of the Company.

The Board of Directors shall have the ultimate responsibility for ensuring that appropriate KYC, AML and CFT standards are implemented and maintained within the Company and that the Company remains compliant with applicable legal and regulatory requirements.

2. OBJECTIVE OF THE POLICY:

The objectives of this Policy are to:

- Prevent the Company from being used, knowingly or unknowingly, for money laundering, terrorist financing or any other unlawful activity.
- Establish a robust framework for customer identification, customer due diligence, ongoing monitoring and reporting of suspicious transactions.
- Ensure that the Company understands its customers, their source of funds, financial behaviour and risk profile.
- Adopt a risk-based approach for identification, assessment and management of money laundering and terrorist financing risks.
- Ensure compliance with the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, RBI (Know Your Customer (KYC)) Directions, 2016 and other applicable regulatory requirements.
- Protect the reputation and integrity of the Company by preventing misuse of its products and services.
- Establish clear responsibilities and accountability for implementation of KYC, AML and CFT requirements across the Company.
- Facilitate timely reporting of prescribed transactions and suspicious activities to FIU-IND and other competent authorities, wherever required.
- Promote a culture of compliance, ethical conduct and regulatory awareness across all levels of the organization.

3. APPLICABILITY

This Policy shall come into effect upon approval by the Board of Directors of the Company and shall remain in force until modified or replaced.

The provisions of this Policy shall apply to all business activities, products, services, delivery channels and customer relationships of the Company, whether existing or introduced in the future.

This Policy shall be applicable to:

- All Directors of the Company;
- All employees, whether permanent, temporary, contractual or outsourced;
- Designated Director and Principal Officer appointed under the PMLA framework;
- Business correspondents, agents, service providers and other persons acting on behalf of the Company, to the extent applicable;
- All customers and prospective customers of the Company.

The Company and its employees shall:

- Comply with the provisions of this Policy and applicable KYC, AML and CFT laws, regulations and guidelines;
- Exercise due diligence while establishing and maintaining customer relationships;
- Promptly identify, investigate and escalate suspicious transactions or activities in accordance with internal procedures;
- Maintain confidentiality of customer information and regulatory reporting processes;
- Cooperate with regulatory, statutory and law enforcement authorities as required under applicable laws.

The Company shall appoint a Designated Director and a Principal Officer in accordance with the requirements of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI (Know Your Customer (KYC)) Directions, 2016.

In case of any inconsistency between this Policy and any applicable law, rule, regulation or regulatory direction, the provisions of such law, rule, regulation or regulatory direction shall prevail.

4. KEY ELEMENTS OF THE POLICY

The Company's KYC framework shall be based on the following key elements:

4.1 Customer Acceptance Policy (CAP)

The Company shall establish and implement a Customer Acceptance Policy laying down the criteria for acceptance of customers and commencement of business relationships.

The Customer Acceptance Policy shall ensure that:

- No customer is accepted anonymously or under a fictitious or benami name.
- No account-based relationship or loan facility is established where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures.
- Customer acceptance decisions are based on the customer's identity, risk profile, source of funds and compliance with applicable laws and regulations.
- Customers are categorized based on risk perception and appropriate due diligence measures are applied accordingly.
- The Company does not open or maintain relationships prohibited under applicable laws, regulations or RBI directions.

4.2 Risk Management

The Company shall adopt a Risk-Based Approach (RBA) for identification, assessment, monitoring and mitigation of Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks.

The Company shall:

- Identify and assess risks arising from customers, products, services, transactions, delivery channels and geographical locations.
- Categorize customers into appropriate risk categories.
- Apply enhanced due diligence measures for higher-risk customers and transactions.
- Periodically review and update its risk assessment framework.

4.3 Customer Identification Procedures (CIP)

The Company shall establish Customer Identification Procedures for verifying the identity of customers and beneficial owners using reliable and independent sources of identification.

The procedures shall include:

- Collection and verification of customer identification information.
- Verification of beneficial ownership, wherever applicable.
- Identification of authorized signatories and persons acting on behalf of customers.
- Verification through documents, digital processes or other methods permitted under applicable regulations.

4.4 Monitoring of Transactions

The Company shall undertake ongoing monitoring of customer relationships and transactions to ensure consistency with the customer's profile, source of funds and declared purpose of the relationship.

The Company shall establish appropriate systems for:

- Identification of unusual or suspicious transactions.
- Monitoring of high-risk customers and transactions.
- Reporting of suspicious transactions and other prescribed reports to FIU-IND and other competent authorities, wherever required.
- Periodic review and updation of customer information and risk categorization.

5. CUSTOMER ACCEPTANCE POLICY (CAP)

The Company shall establish and implement a Customer Acceptance Policy (CAP) that lays down the criteria for acceptance of customers and commencement of business relationships in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016.

The Customer Acceptance Policy shall ensure that:

- No customer is accepted in an anonymous, fictitious or benami name.
- No business relationship is established unless the customer due diligence requirements prescribed under applicable laws and regulations are satisfactorily completed.
- Customer acceptance decisions are based on the customer's identity, risk profile, source of funds and compliance with applicable regulatory requirements.
- Customers are categorized into appropriate risk categories based on the Company's risk assessment framework.
- Enhanced due diligence measures are applied in respect of customers classified as high risk.
- The Company does not knowingly enter into relationships with persons or entities prohibited under applicable laws, sanctions regulations or regulatory directions.
- Customer acceptance procedures do not result in denial of financial services to any person solely on the basis of low income, social status or other prohibited grounds.

Where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures, establish the identity of the customer or beneficial owner, or obtain information required under applicable laws and regulations, the Company shall not establish the business relationship or shall take such action as may be permissible under applicable laws and regulatory guidelines.

The Company shall adopt a Risk-Based Approach while onboarding customers and shall apply Customer Due Diligence measures commensurate with the level of risk associated with the customer.

5.1 Customer Acceptance Criteria

The Company shall establish a business relationship only after undertaking appropriate Customer Due Diligence (CDD) measures and satisfying itself about the identity and legitimacy of the customer.

The Company shall ensure that:

- Sufficient information is obtained to identify the customer and verify the customer's identity.
- The purpose and intended nature of the business relationship are understood.

- The customer is not included in any sanctions list, prohibited list or other list prescribed under applicable laws and regulations.
- Appropriate information relating to the customer's occupation, source of funds, source of income and other relevant details is obtained, wherever required.
- The level of Customer Due Diligence is commensurate with the customer's risk profile.

The Company shall not establish or continue a business relationship where:

- The customer fails or refuses to provide information or documents required for Customer Due Diligence.
- The Company is unable to verify the identity of the customer or beneficial owner.
- The information provided by the customer appears to be false, misleading or inconsistent.
- The proposed relationship gives rise to concerns regarding money laundering, terrorist financing, fraud or any other unlawful activity.

The Company may decline onboarding of any customer where the risks associated with the relationship cannot be adequately managed in accordance with applicable laws, regulations and internal policies.

5.2 Risk Categorisation of Customers

The Company shall adopt a Risk-Based Approach (RBA) for categorisation of customers based on the perceived Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks associated with the customer.

The risk categorisation shall be based on various factors including:

- Nature of the customer and occupation.
- Source of income and source of funds.
- Geographical location of the customer.
- Products and services availed.
- Mode of onboarding and delivery channel.
- Transaction pattern and expected account behaviour.
- Any other risk indicators considered relevant by the Company.
- Loan product availed by the customer, including payday loans and EMI-based loans.
- Repayment behaviour and borrowing patterns of the customer.
- Frequency of loan applications and borrowing activity.

Based on the risk assessment, customers may be classified into the following categories:

Low Risk

Customers whose identity and source of income can be easily verified and who present a lower risk of money laundering or terrorist financing. Examples may include salaried individuals employed with reputed organizations, government employees and other customers assessed as low risk by the Company.

Medium Risk

Customers who do not fall under either low-risk or high-risk categories and require standard monitoring and due diligence measures.

High Risk

Customers who, by virtue of their profile, occupation, source of funds, geographical location, transaction pattern or other risk factors, are considered to present a higher risk of money laundering or terrorist financing.

The following categories may generally be classified as high-risk customers:

- Politically Exposed Persons (PEPs).
- Non-face-to-face customers.
- Customers from high-risk jurisdictions identified by competent authorities.
- Customers having complex ownership structures.
- Customers whose source of funds or source of wealth cannot be easily verified.
- Any other customer category identified by the Company as high risk.

The risk categorisation of customers shall be reviewed periodically and may be revised based on updated customer information, transaction behaviour, regulatory requirements or risk assessment findings.

The Company shall apply Customer Due Diligence and monitoring measures commensurate with the risk category assigned to the customer.

5.3 Customer Due Diligence (CDD)

The Company shall undertake Customer Due Diligence (CDD) before establishing a business relationship with a customer and at such other times as may be required under applicable laws, regulations and RBI directions.

The Company shall identify and verify the identity of the customer and, where applicable, the beneficial owner, using reliable and independent sources of identification.

The Customer Due Diligence process shall include:

- Identification and verification of the customer.
- Obtaining and verifying Permanent Account Number (PAN) or Form 60, wherever applicable.
- Verification of the customer's address through Officially Valid Documents (OVDs) or such other documents permitted under applicable regulations.
- Obtaining information regarding the purpose and intended nature of the business relationship.
- Identification and verification of beneficial owners, wherever applicable.
- Verification of the identity of persons acting on behalf of customers and obtaining proof of authorization.
- Screening of customers against applicable sanctions lists and regulatory restrictions, wherever required.

The Company may undertake Customer Due Diligence through physical onboarding, Digital KYC, Aadhaar Offline Verification, Video-based Customer Identification Process (V-CIP), CKYCR records or any other mode permitted under applicable laws and RBI directions.

The Company shall not establish a business relationship or disburse any loan where the Customer Due Diligence requirements cannot be satisfactorily completed.

Where the Company is unable to complete Customer Due Diligence, or where the information provided by the customer is found to be incomplete, inconsistent or unreliable, the Company may decline the application, discontinue the business relationship or take such action as may be permissible under applicable laws and regulatory requirements.

Customer Due Diligence records and related information shall be maintained in accordance with applicable record retention requirements.

5.4 Customer Identification Procedure (CIP)

The Company shall establish and implement a Customer Identification Procedure (CIP) for verifying the identity of customers and beneficial owners in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016 and other applicable regulatory requirements.

The Customer Identification Procedure shall enable the Company to:

- Identify the customer and verify the customer's identity using reliable and independent sources of identification.
- Identify and verify the beneficial owner, wherever applicable.

- Verify the identity of persons acting on behalf of customers and obtain proof of authorization.
- Understand the nature and purpose of the business relationship.

The Company may undertake customer identification through any mode permitted under applicable laws and regulatory guidelines, including:

- Physical KYC.
- Digital KYC.
- Aadhaar Offline Verification.
- Video-based Customer Identification Process (V-CIP).
- Equivalent e-documents.
- Central KYC Records Registry (CKYCR) records.
- Any other method permitted by RBI from time to time.

The Company shall obtain and verify such documents, information and declarations as may be required under applicable laws and RBI directions for establishing the identity of the customer.

Where the customer is a legal entity, the Company shall identify and verify the legal entity, its authorized signatories and beneficial owners in accordance with applicable regulatory requirements.

The Company shall ensure that customer identification records are maintained accurately and updated periodically in accordance with the requirements of applicable laws and regulations.

5.5 Identification of Beneficial Owner

The Company shall identify and verify the Beneficial Owner(s) in respect of customers that are legal persons or legal arrangements, in accordance with the provisions of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI (Know Your Customer (KYC)) Directions, 2016.

The Company shall take reasonable measures to understand the ownership and control structure of the customer and determine the natural person(s) who ultimately own, control or exercise effective control over the customer.

For identification of Beneficial Owners, the Company shall obtain such information and documents as may be prescribed under applicable laws and regulatory guidelines.

The Company shall verify the identity of the Beneficial Owner using reliable and independent sources of identification and maintain appropriate records thereof.

Where no natural person is identified as the Beneficial Owner, the Company shall identify the natural person holding the position of senior managing official in accordance with applicable regulatory requirements.

The Company may obtain declarations, ownership charts, constitutional documents and such other information as may be necessary to identify and verify the Beneficial Owner.

The Company shall periodically review beneficial ownership information and update its records whenever there is a change in ownership, control or other relevant information relating to the customer.

Where the Company is unable to identify or verify the Beneficial Owner to its satisfaction, it may decline to establish the business relationship or take such action as may be permissible under applicable laws and regulatory requirements.

5.6 Enhanced Due Diligence (EDD)

The Company shall apply Enhanced Due Diligence (EDD) measures in respect of customers, transactions and business relationships assessed as high risk under its Risk-Based Approach.

Enhanced Due Diligence may be undertaken in respect of, inter alia:

- Politically Exposed Persons (PEPs).
- Non-face-to-face customers.
- Customers from high-risk jurisdictions.
- Customers having complex ownership structures.
- Customers whose source of funds or source of wealth cannot be readily established.
- Customers involved in high-value or unusual transactions.
- Any other customer category identified by the Company as high risk.

The Enhanced Due Diligence measures may include:

- Obtaining additional identity, financial or business-related information.
- Obtaining information regarding source of funds and source of wealth, wherever considered necessary.
- Enhanced scrutiny of customer onboarding and transactions.
- Obtaining approval from an appropriate authority within the Company before establishing or continuing the relationship, wherever required.
- More frequent review and updation of customer information.
- Enhanced transaction monitoring and ongoing due diligence.

The extent of Enhanced Due Diligence shall be commensurate with the level of risk identified and shall be reviewed periodically by the Company.

The Company may decline to establish, continue or renew a business relationship where the risks associated with the customer cannot be adequately mitigated or managed.

5.7 Simplified Due Diligence (SDD)

The Company may apply Simplified Due Diligence measures in respect of customers assessed as low risk, subject to compliance with applicable laws, regulatory requirements and the RBI (Know Your Customer (KYC)) Directions, 2016.

Simplified Due Diligence shall be applied only where the lower risk has been established through the Company's risk assessment process and where such application is permitted under applicable regulatory requirements.

While applying Simplified Due Diligence, the Company shall ensure that:

- Sufficient information is obtained to identify and verify the customer.
- The customer is appropriately classified as low risk.
- Adequate monitoring of the business relationship is carried out on an ongoing basis.
- Simplified Due Diligence is not applied where there are suspicions of money laundering, terrorist financing or any other unlawful activity.
- Simplified Due Diligence does not result in non-compliance with any requirement prescribed under applicable laws, regulations or RBI directions.

The Company shall apply Customer Due Diligence measures commensurate with the risks associated with the customer and may discontinue Simplified Due Diligence where the customer's risk profile changes or additional risk factors are identified.

5.8 Politically Exposed Persons (PEPs)

The Company shall establish appropriate risk management systems for determining whether a customer or beneficial owner is a Politically Exposed Person (PEP).

Where a customer or beneficial owner is identified as a PEP, the Company shall:

- Undertake Enhanced Due Diligence measures.
- Obtain approval from Senior Management before establishing or continuing the business relationship.

- Take reasonable measures to establish the source of funds and source of wealth, wherever considered necessary.
- Conduct enhanced ongoing monitoring of the business relationship and transactions.

Where an existing customer subsequently becomes a PEP, the relationship shall be subjected to enhanced review and appropriate approval shall be obtained for continuation of the relationship.

The Company shall apply a risk-based approach while dealing with PEPs and shall undertake such additional measures as may be required under applicable laws, regulations and RBI directions.

The identification of a customer as a PEP shall not by itself result in denial of services, provided the Company is satisfied that the risks associated with the relationship can be appropriately managed and monitored.

5.9 Non-Face-to-Face Customers

The Company may establish business relationships with customers through non-face-to-face modes in accordance with applicable laws, regulations and RBI directions.

The Company shall implement appropriate policies, procedures and controls to manage the risks associated with non-face-to-face customer onboarding and transactions.

In respect of non-face-to-face customers, the Company shall:

- Apply Customer Due Diligence measures in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016.
- Undertake additional verification and due diligence measures, wherever considered necessary.
- Ensure that the customer's identity is verified through permitted modes and reliable sources of identification.
- Apply Enhanced Due Diligence measures where the customer is assessed as high risk.
- Subject such relationships to enhanced monitoring based on the risk profile of the customer.
- Establish appropriate controls to prevent identity theft, impersonation, fraud and misuse of the onboarding process.

The Company shall adopt a risk-based approach while onboarding non-face-to-face customers and may prescribe additional safeguards as may be considered

necessary based on the nature of the product, customer profile and associated risks.

The Company may decline to establish or continue a business relationship where it is unable to satisfactorily verify the identity of the customer or where the risks associated with the relationship cannot be adequately managed.

5.10 Video-based Customer Identification Process (V-CIP)

The Company may undertake customer onboarding through Video-based Customer Identification Process (V-CIP) in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016 and such other guidelines as may be issued by the Reserve Bank of India from time to time.

Where V-CIP is adopted, the Company shall establish appropriate systems, procedures, controls and technological safeguards to ensure secure and effective customer identification.

The Company shall ensure that:

- V-CIP is conducted only through secure and RBI-compliant processes and infrastructure.
- The identity of the customer is verified through the documents, information and procedures prescribed under applicable regulations.
- Appropriate measures are implemented to prevent identity theft, impersonation, fraud and unauthorized access.
- Records of the V-CIP process are maintained in accordance with applicable legal and regulatory requirements.
- Appropriate audit trails and monitoring mechanisms are maintained.

The Company shall periodically review the adequacy and effectiveness of the V-CIP framework and implement necessary improvements based on regulatory requirements, technological developments and risk assessments.

The Company may suspend, discontinue or reject onboarding through V-CIP where the customer's identity cannot be satisfactorily verified or where any discrepancy, anomaly or risk indicator is identified during the process.

6. ML/TF AND PF RISK MANAGEMENT

The Company shall establish and maintain a comprehensive framework for identification, assessment, monitoring and mitigation of risks relating to Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) in accordance with applicable

laws, regulatory requirements and the RBI (Know Your Customer (KYC)) Directions, 2016.

6.1 Risk-Based Approach

The Company shall adopt a Risk-Based Approach (RBA) for managing ML, TF and PF risks associated with its customers, products, services, delivery channels and geographical locations.

The risk assessment framework shall enable the Company to:

- Identify and assess ML, TF and PF risks.
- Understand the nature and level of risks associated with its business activities.
- Apply appropriate risk mitigation measures.
- Allocate resources commensurate with the level of identified risks.

6.2 Enterprise-Wide Risk Assessment

The Company shall undertake an enterprise-wide assessment of ML, TF and PF risks and document the results thereof.

The assessment shall consider, inter alia:

- Nature and size of the Company's business.
- Customer profiles and risk characteristics.
- Products and services offered by the Company.
- Delivery and distribution channels.
- Geographical locations of customers and operations.
- Emerging risks and typologies identified by regulators and competent authorities.
- Risks arising from digital onboarding, payday loan products, short-tenure lending products and EMI-based lending products.

6.3 Review of Risk Assessment

The ML, TF and PF Risk Assessment shall be reviewed periodically and updated whenever there are material changes in the Company's business, products, services, customer base, regulatory requirements or risk environment.

6.4 Risk Mitigation Measures

Based on the outcome of the risk assessment, the Company shall implement appropriate controls and mitigation measures, including:

- Customer Due Diligence and Enhanced Due Diligence measures.
- Transaction monitoring mechanisms.

- Customer risk categorisation.
- Employee training and awareness programmes.
- Internal controls and compliance monitoring.

6.5 Board and Senior Management Oversight

The Board of Directors and Senior Management shall ensure that adequate systems, procedures and controls are established for effective management of ML, TF and PF risks.

The Board shall periodically review the effectiveness of the Company's risk management framework and provide necessary guidance for strengthening the same.

6.6 Documentation and Record Maintenance

The Company shall maintain appropriate documentation relating to its ML, TF and PF Risk Assessment, methodology, findings, reviews and mitigation measures and shall make the same available to regulatory or statutory authorities, whenever required.

7. CUSTOMER DUE DILIGENCE PROCEDURES FOR INDIVIDUAL CUSTOMERS

The Company shall undertake Customer Due Diligence (CDD) before establishing a business relationship with an individual customer and at such other times as may be prescribed under applicable laws and regulatory requirements.

7.1 Identification and Verification of Individual Customers

The Company shall identify and verify the identity of individual customers using reliable and independent sources of identification in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016.

Customer identification may be carried out through:

- Aadhaar Offline Verification;
- Digital KYC;
- Video-based Customer Identification Process (V-CIP);
- Equivalent e-documents;
- Central KYC Records Registry (CKYCR) records; or
- Any other mode permitted under applicable laws and RBI directions.

7.2 Permanent Account Number (PAN)

The Company shall obtain and verify the Permanent Account Number (PAN) or Form 60, as applicable, in accordance with the provisions of applicable laws and regulatory requirements.

7.3 Officially Valid Documents (OVDs)

The Company shall obtain and verify such Officially Valid Documents (OVDs) and other documents as may be prescribed under the RBI (Know Your Customer (KYC)) Directions, 2016 for establishing the identity and address of the customer.

Where the OVD furnished by the customer does not contain the current address, the Company may obtain such additional documents or declarations as may be permitted under applicable regulatory requirements.

7.4 Customer Information

The Company may obtain such information as may be necessary for undertaking Customer Due Diligence and risk assessment, including:

- Full name;
- Date of birth;
- Address;
- Mobile number;
- E-mail address, where available;
- Occupation or employment details;
- Source of income and source of funds, wherever required;
- Employment details, salary information or other income-related information, as applicable.
- Bank account details and repayment information, wherever required for credit assessment and regulatory compliance purposes.
- Any other information considered necessary for compliance with applicable laws and regulations.

7.5 Purpose of Relationship

The Company shall obtain information regarding the purpose and intended nature of the business relationship and assess whether the proposed relationship is consistent with the customer's profile and risk category.

7.6 Existing Customers

The Company shall carry out periodic updation of KYC records and Customer Due Diligence information of existing customers in accordance with applicable laws, RBI directions and internal policies.

7.7 Inability to Complete Customer Due Diligence

Where the Company is unable to complete Customer Due Diligence requirements to its satisfaction, it may decline the customer's application, suspend processing of the application or take such other action as may be permissible under applicable laws and regulatory requirements.

8. CUSTOMER DUE DILIGENCE FOR PROPRIETORSHIP CONCERNS

Where the customer is a proprietorship concern, the Company shall undertake Customer Due Diligence in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016.

In addition to identifying and verifying the identity of the proprietor, the Company shall obtain such documents and information as may be required to establish the existence and business activity of the proprietorship concern.

The Company shall obtain and verify such documents, licenses, registrations, certificates or other records as may be prescribed under applicable laws and RBI directions from time to time.

The Company may obtain additional information or documents wherever considered necessary based on the risk profile of the customer.

9. CUSTOMER DUE DILIGENCE FOR LEGAL ENTITIES

Where the customer is a legal entity, the Company shall undertake Customer Due Diligence in accordance with applicable laws, regulatory requirements and RBI directions.

The Company shall identify and verify:

- The legal entity;
- Persons authorised to act on behalf of the legal entity;
- Beneficial Owner(s), wherever applicable; and
- Such other persons as may be required under applicable laws and regulations.

The Company shall obtain constitutional documents, authorization documents and such other information as may be necessary for identification and verification of the legal entity and its authorised representatives.

The Company may seek additional information and documentation based on the nature of the entity, ownership structure and risk profile.

10. BENEFICIAL OWNERSHIP REQUIREMENTS

The Company shall identify and verify the Beneficial Owner(s) of legal entities and legal arrangements in accordance with the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI (Know Your Customer (KYC)) Directions, 2016.

The Company shall take reasonable measures to understand the ownership and control structure of the customer and identify the natural person(s) exercising ownership, control or effective control over the customer.

Where no natural person is identified as the Beneficial Owner, the Company shall identify the natural person holding the position of senior managing official in accordance with applicable regulatory requirements.

The Company shall maintain records relating to identification and verification of Beneficial Owners and update such records whenever material changes are identified.

11. ONGOING DUE DILIGENCE AND MONITORING OF TRANSACTIONS

The Company shall undertake ongoing due diligence of customer relationships and monitor transactions to ensure that they are consistent with the customer's profile, source of funds, risk category and the nature of the business relationship.

11.1 Ongoing Due Diligence

The Company shall conduct ongoing due diligence throughout the course of the customer relationship and shall periodically review customer information, risk categorisation and transaction behaviour.

The extent and frequency of ongoing due diligence shall be commensurate with the risk profile of the customer.

11.2 Monitoring of Transactions

The Company shall establish appropriate systems and procedures for monitoring customer transactions and identifying unusual, suspicious or potentially high-risk activities.

Particular attention shall be paid to:

- Complex or unusually large transactions;
- Transactions that have no apparent economic or lawful purpose;
- Transactions inconsistent with the customer's profile or known source of income;
- Unusual transaction patterns or activities;
- Frequent loan applications or repetitive borrowing patterns inconsistent with the customer's known profile.

- Unusual repayment patterns, early closures, multiple loan rollovers or other activities that may indicate elevated money laundering or fraud risks.
- Transactions involving multiple accounts or repayment sources that appear inconsistent with the customer's profile.
- Transactions involving high-risk customers or jurisdictions; and
- Any activity that may give rise to suspicion of money laundering, terrorist financing or other unlawful conduct.

11.3 Enhanced Monitoring

Customers classified as high risk shall be subject to enhanced monitoring and more frequent review.

The Company may seek additional information, documents or explanations from customers where considered necessary for risk assessment or regulatory compliance purposes.

11.4 Review of Customer Information

The Company shall periodically review and update customer identification records, KYC information and risk categorisation in accordance with applicable laws, RBI directions and internal policies.

11.5 Suspicious Transactions

Where any transaction or activity appears unusual, suspicious or inconsistent with the customer's profile, the same shall be examined and escalated in accordance with the Company's internal procedures and applicable regulatory requirements.

The Company shall maintain appropriate records of such reviews and actions taken thereon.

12. PERIODIC UPDATION OF KYC

The Company shall periodically update customer identification records and KYC information in accordance with the RBI (Know Your Customer (KYC)) Directions, 2016 and other applicable regulatory requirements.

12.1 Periodic Updation

Periodic updation shall be carried out based on the risk categorisation of the customer as under:

Risk Category	Periodicity
----------------------	--------------------

High Risk	At least once every 2 years
Medium Risk	At least once every 8 years
Low Risk	At least once every 10 years

The above periodicity shall be subject to such modifications as may be prescribed by RBI from time to time.

12.2 Updation of Customer Information

The Company may obtain and update:

- Customer identification information;
- Address details;
- Contact information;
- PAN or equivalent identification details;
- Beneficial ownership information, wherever applicable;
- Risk profile and other relevant information.

The Company may update KYC records through physical, digital or such other modes as may be permitted under applicable laws and RBI directions.

12.3 Change in Customer Information

Customers shall promptly notify the Company of any material change in information or documents furnished during the onboarding process.

Upon receipt of such information, the Company may obtain supporting documents and update its records accordingly.

12.4 Enhanced Review

The Company may undertake earlier or more frequent updation of KYC records in respect of high-risk customers, suspicious accounts, customers subject to enhanced due diligence or where considered necessary based on risk assessment.

12.5 Non-Compliance with KYC Updation Requirements

Where a customer fails to comply with periodic KYC updation requirements despite appropriate notices and follow-up, the Company may take such measures as may be permissible under applicable laws, RBI directions and internal policies.

13. CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company shall comply with the requirements relating to the Central KYC Records Registry (CKYCR) in accordance with the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI (Know Your Customer (KYC)) Directions, 2016.

13.1 Upload of KYC Records

The Company shall upload customer KYC records to CKYCR within the timelines prescribed under applicable laws and regulatory requirements.

13.2 KYC Identifier

Upon generation of a KYC Identifier by CKYCR, the Company shall communicate the KYC Identifier to the customer in such manner as may be prescribed under applicable regulations.

13.3 Retrieval of KYC Records

The Company may retrieve KYC records from CKYCR using the customer's KYC Identifier and may rely on such records in accordance with applicable laws and RBI directions.

13.4 Updation of CKYCR Records

Where there is a change in customer information or KYC records, the Company shall update the records with CKYCR within the timelines prescribed under applicable laws and regulatory requirements.

13.5 Compliance and Record Maintenance

The Company shall establish appropriate systems and controls to ensure timely uploading, retrieval, updation and maintenance of KYC records with CKYCR.

The Company shall maintain records relating to CKYCR uploads, downloads, updates and related communications in accordance with applicable legal and regulatory requirements.

14. APPOINTMENT OF DESIGNATED DIRECTOR AND PRINCIPAL OFFICER

The Company shall appoint a Designated Director and a Principal Officer in accordance with the requirements of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI (Know Your Customer (KYC)) Directions, 2016.

14.1 Designated Director

The Board of Directors shall designate a Director as the Designated Director for ensuring overall compliance with the obligations imposed under the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder.

The Designated Director shall be responsible for:

- Ensuring compliance with applicable KYC, AML and CFT requirements.
- Overseeing implementation of the Company's KYC/AML/CFT framework.
- Ensuring that appropriate internal controls, systems and procedures are established and maintained.
- Reviewing significant compliance issues relating to KYC, AML and CFT matters.
- Providing guidance and support for strengthening the Company's compliance framework.

14.2 Principal Officer

The Company shall appoint a Principal Officer at the management level who shall be responsible for monitoring and managing compliance with the obligations prescribed under the Prevention of Money Laundering Act, 2002 and applicable regulatory requirements.

The Principal Officer shall be responsible for:

- Monitoring compliance with KYC, AML and CFT requirements.
- Receiving, reviewing and evaluating alerts, unusual activities and suspicious transactions.
- Ensuring submission of reports to FIU-IND and other competent authorities, wherever required.
- Coordinating with regulatory, statutory and law enforcement authorities.
- Providing guidance and support to employees on KYC, AML and CFT matters.
- Maintaining records relating to regulatory reporting and compliance activities.

14.3 Reporting and Escalation

The Principal Officer shall report material KYC, AML and CFT matters to the Designated Director and Senior Management, wherever required.

The Designated Director and Principal Officer shall have adequate authority, resources and access to information necessary for effective discharge of their responsibilities under applicable laws and regulatory requirements.

14.4 Intimation to Regulatory Authorities

The Company shall communicate the details of the Designated Director and Principal Officer to the appropriate regulatory and statutory authorities in accordance with applicable laws and regulatory requirements and shall promptly update such information whenever changes occur.

15. RECORD RETENTION AND PRESERVATION OF DOCUMENTS

The Company shall maintain and preserve records in accordance with the requirements of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI (Know Your Customer (KYC)) Directions, 2016.

15.1 Maintenance of Records

The Company shall maintain records of:

- Customer identification and verification documents obtained during Customer Due Diligence.
- Account files, loan records and business correspondence.
- Transaction records and related information.
- Beneficial ownership information, wherever applicable.
- Suspicious transaction reviews, investigations and regulatory reporting records.
- Such other records as may be required under applicable laws and regulatory requirements.

15.2 Preservation of Records

The Company shall preserve:

- Records relating to transactions for a minimum period of five years from the date of transaction.
- Records relating to customer identification and Customer Due Diligence for a minimum period of five years after the end of the business relationship with the customer or closure of the account, whichever is later.

The retention period shall be subject to any longer period prescribed under applicable laws, regulatory requirements or directions issued by competent authorities.

15.3 Availability of Records

The Company shall ensure that records are readily available and can be retrieved in a timely manner whenever required by:

- Reserve Bank of India;

- Financial Intelligence Unit – India (FIU-IND);
- Law enforcement agencies;
- Statutory authorities; or
- Any other competent authority.

15.4 Form of Preservation

Records may be maintained in physical form, electronic form or such other form as may be permitted under applicable laws and regulatory requirements, provided that the integrity, confidentiality and accessibility of such records are maintained.

15.5 Confidentiality of Records

The Company shall implement appropriate safeguards to ensure confidentiality, security and protection of customer information and records from unauthorized access, disclosure, alteration or destruction.

16. REPORTING OF TRANSACTIONS

The Company shall comply with all reporting obligations prescribed under the Prevention of Money Laundering Act, 2002, the Rules framed thereunder, the RBI (Know Your Customer (KYC)) Directions, 2016 and other applicable regulatory requirements.

16.1 Reporting to FIU-IND

The Company shall furnish prescribed reports to the Financial Intelligence Unit – India (FIU-IND) within the timelines and in the manner specified under applicable laws and regulations.

16.2 Suspicious Transaction Reports (STRs)

Where the Company knows, suspects or has reasonable grounds to suspect that a transaction or attempted transaction involves proceeds of crime, money laundering, terrorist financing or any other unlawful activity, the same shall be examined and reported to FIU-IND in accordance with applicable legal and regulatory requirements.

The Company shall maintain appropriate procedures for identification, investigation, escalation and reporting of suspicious transactions.

16.3 Cash Transaction Reports (CTRs)

The Company shall report cash transactions and cash-related activities, wherever applicable, in accordance with the requirements prescribed under the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder.

16.4 Other Regulatory Reports

The Company shall submit such other reports, statements, information and disclosures as may be required by FIU-IND, RBI or any other competent authority from time to time.

16.5 Internal Escalation Mechanism

Employees shall promptly report any unusual, suspicious or potentially reportable activity to the Principal Officer through the prescribed internal reporting mechanism.

The Principal Officer shall review such cases and determine the appropriate course of action in accordance with applicable laws and regulatory requirements.

16.6 Confidentiality of Reporting

The fact that a Suspicious Transaction Report (STR) or any related information has been filed or is proposed to be filed with FIU-IND shall be kept strictly confidential.

No employee, officer, director or other person shall disclose, directly or indirectly, the existence or contents of any STR or related investigation except as permitted under applicable laws and regulatory requirements.

16.7 Record Maintenance

The Company shall maintain appropriate records relating to internal reviews, investigations, escalations and regulatory reporting undertaken under this Policy in accordance with applicable record retention requirements.

17. SANCTIONS SCREENING AND COMPLIANCE WITH UNSC RESOLUTIONS

The Company shall establish and maintain appropriate systems and procedures to ensure compliance with applicable sanctions requirements, directions issued by the Government of India and the Reserve Bank of India, and the obligations relating to targeted financial sanctions under the United Nations Security Council (UNSC) Resolutions.

17.1 Sanctions Screening

The Company shall undertake appropriate screening of customers, beneficial owners and other relevant parties against applicable sanctions lists and watchlists as prescribed under applicable laws and regulatory requirements.

The screening shall be carried out:

- At the time of customer onboarding;
- During periodic updation of KYC records;
- Upon changes in customer information;
- As part of ongoing monitoring processes; and
- At such other intervals as may be considered necessary by the Company.

17.2 Compliance with UNSC Resolutions

The Company shall comply with the obligations relating to targeted financial sanctions and other measures prescribed under the relevant UNSC Resolutions adopted by the Government of India and applicable regulatory authorities.

The Company shall take such actions as may be required under applicable laws and regulatory guidelines in respect of persons, entities or organizations appearing in designated sanctions lists.

17.3 Monitoring and Escalation

Where a potential match or confirmed match is identified during sanctions screening, the matter shall be promptly escalated to the Principal Officer for review and appropriate action.

The Company shall maintain documented procedures for investigation, escalation and reporting of sanctions-related alerts.

17.4 Reporting Obligations

The Company shall make such filings, reports, notifications and disclosures as may be required by FIU-IND, RBI, Government authorities or any other competent authority in relation to sanctions compliance.

17.5 Record Maintenance

The Company shall maintain appropriate records relating to sanctions screening, alerts, investigations, decisions and regulatory reporting in accordance with applicable legal and regulatory requirements.

18. EMPLOYEE TRAINING AND AWARENESS

The Company shall establish an ongoing training and awareness programme to ensure effective implementation of the KYC, AML and CFT framework.

18.1 Training Programme

The Company shall provide appropriate training to its employees on:

- The provisions of the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder.
- RBI (Know Your Customer (KYC)) Directions, 2016 and other applicable regulatory requirements.
- Customer Due Diligence (CDD) requirements.
- Identification and reporting of suspicious transactions.
- Sanctions screening and proliferation financing requirements.
- Internal policies, procedures and reporting mechanisms.

18.2 Periodic Awareness Programmes

The Company shall conduct periodic awareness programmes to keep employees informed about:

- Changes in laws, regulations and regulatory expectations.
- Emerging money laundering and terrorist financing typologies.
- Internal compliance requirements and best practices.

18.3 Training for New Employees

Appropriate induction training on KYC, AML and CFT requirements shall be provided to new employees and other relevant personnel as part of the onboarding process.

18.4 Role-Based Training

The Company may provide specialised training to employees handling customer onboarding, operations, compliance, risk management, transaction monitoring and regulatory reporting functions.

18.5 Training Records

The Company shall maintain appropriate records of training programmes, attendance and awareness initiatives conducted under this Policy.

19. INTERNAL CONTROL, AUDIT AND COMPLIANCE REVIEW

The Company shall establish adequate internal control mechanisms to ensure effective implementation of the KYC, AML, CFT and Proliferation Financing (PF) framework and compliance with applicable laws and regulatory requirements.

19.1 Internal Control Framework

The Company shall maintain appropriate internal controls, systems and procedures for:

- Customer onboarding and Customer Due Diligence (CDD);
- Ongoing monitoring of customer relationships and transactions;
- Detection and reporting of suspicious transactions;
- Sanctions screening and compliance;
- Record maintenance and regulatory reporting; and
- Compliance with applicable KYC, AML and CFT requirements.

19.2 Independent Review and Audit

The implementation and effectiveness of the KYC, AML and CFT framework shall be subject to periodic review by the Internal Audit function or any other independent review mechanism established by the Company.

The scope of such review may include:

- Compliance with applicable laws and regulatory requirements;
- Adequacy of policies, procedures and internal controls;
- Customer onboarding and due diligence processes;
- Transaction monitoring and reporting mechanisms;
- Record maintenance and documentation requirements; and
- Effectiveness of employee awareness and training programmes.

19.3 Compliance Monitoring

The Compliance function shall periodically monitor adherence to the requirements of this Policy and applicable regulatory requirements.

Material observations, deficiencies or instances of non-compliance shall be reported to Senior Management and the Board of Directors, wherever considered necessary.

19.4 Corrective and Remedial Measures

Appropriate corrective and remedial measures shall be implemented in respect of deficiencies identified through internal reviews, audits, compliance monitoring activities or regulatory inspections.

The implementation status of corrective actions shall be monitored and reviewed periodically.

19.5 Regulatory Inspection

The Company shall extend full cooperation to the Reserve Bank of India, FIU-IND and other competent authorities during inspections, audits, examinations or investigations and shall provide such information, records and documents as may be required under applicable laws and regulations.

20. CUSTOMER EDUCATION AND AWARENESS

The Company shall take appropriate measures to educate customers regarding the requirements of KYC, AML and CFT regulations and the importance of providing accurate and updated information.

The Company may disseminate information through its website, mobile application, customer communications and other appropriate channels regarding:

- KYC requirements and documentation;
- Periodic updation of KYC records;
- Customer rights and responsibilities;
- Grievance redressal mechanisms; and
- Other regulatory requirements applicable to customers.

The Company shall endeavour to create awareness amongst customers regarding fraudulent practices, identity theft, phishing and other activities that may adversely affect the security of customer information and financial transactions.

21. CONFIDENTIALITY AND DATA PROTECTION

The Company shall maintain confidentiality of customer information obtained during the course of Customer Due Diligence, ongoing monitoring and other business activities.

Customer information shall be used only for legitimate business, regulatory and legal purposes and shall not be disclosed except:

- With the consent of the customer;
- Where disclosure is required under applicable laws or regulations;
- Pursuant to directions of a court, regulatory authority or competent government authority; or
- For reporting obligations under applicable laws.

The Company shall implement appropriate administrative, technical and operational safeguards to protect customer information against unauthorized access, disclosure, alteration, misuse, loss or destruction.

All employees, agents, service providers and other persons having access to customer information shall maintain strict confidentiality and comply with applicable data protection and information security requirements.

22. POLICY REVIEW AND AMENDMENTS

This Policy shall be reviewed periodically by the Board of Directors and may be amended, modified or revised as may be considered necessary to ensure continued compliance with applicable laws, regulatory requirements and business needs.

Any changes in the Prevention of Money Laundering Act, 2002, the Rules framed thereunder, RBI (Know Your Customer (KYC)) Directions, 2016, FIU-IND guidelines or any other applicable laws and regulations shall be appropriately incorporated into this Policy.

23. REGULATORY OVERRIDE

In the event of any inconsistency between the provisions of this Policy and any applicable law, rule, regulation, circular, notification or direction issued by the Reserve Bank of India, FIU-IND or any other competent authority, the provisions of such law, rule, regulation, circular, notification or direction shall prevail.

Any matter not specifically covered under this Policy shall be governed by the provisions of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder, RBI (Know Your Customer (KYC)) Directions, 2016 and other applicable laws, regulations and guidelines, as amended from time to time.