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

1. Introduction

This Know Your Customer (KYC) Policy and Anti-Money Laundering (AML) Standards document outlines the framework for Praveen Capital Private Limited (PCPL) to prevent its financial services from being used for money laundering (ML), terrorist financing (TF), fraud, or other illicit activities. It is formulated in strict compliance with:

- The Prevention of Money Laundering Act, 2002 (PMLA), as amended from time to time.
- The Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time.
- All circulars, guidelines, and Master Directions issued by the Reserve Bank of India (RBI) regarding Know Your Customer (KYC) norms, Anti-Money Laundering (AML), and Combating Financing of Terrorism (CFT), including the latest "Master Direction – Know Your Customer (KYC) Direction, 2016", as updated.
- Relevant directives from other statutory/regulatory authorities applicable to [Your NBFC Name].

The objective of this policy is to enable PCPL to:

- Have a clear Customer Acceptance Policy (CAP).
- Establish robust Customer Identification Procedures (CIP).
- Implement effective ongoing monitoring of transactions and customer relationships.
- Manage money laundering and terrorist financing risks prudently.
- Report suspicious transactions to the Financial Intelligence Unit - India (FIU-IND) as required.

2. Scope and Applicability

This policy applies to all existing and prospective customers of PCPL, across all its products, services, branches, and delivery channels. It covers:

- All account-based relationships (e.g., loans, deposits, investments).
- Occasional transactions, including single transactions or a series of connected transactions, of an amount equal to or exceeding ₹50,000, whether conducted as a single transaction or several transactions that appear to be connected.
- Any international money transfer operations.
- When there is a doubt about the authenticity or adequacy of previously obtained customer identification data.

This policy applies to all employees, directors, agents, and third-party service providers acting on behalf of PCPL .

3. Definitions

- Customer: A person who is engaged in a financial transaction or activity with PCPL and includes a person on whose behalf the person who is engaged in the transaction or activity is acting. This includes individuals, Hindu Undivided Families (HUFs), companies, partnership firms, trusts, unincorporated associations, body of individuals, and artificial juridical persons.
- Customer Due Diligence (CDD): The process of identifying and verifying the identity of the customer and the beneficial owner, understanding the purpose and intended nature of the business relationship, and conducting ongoing due diligence on the business relationship.
- Beneficial Owner (BO): The natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction or activity is being conducted. (Specific thresholds as per PMLA Rules - refer to Section 5.2.4 for details).
- Officially Valid Document (OVD): As defined under the PMLA Rules, these are specific documents accepted for identity and address verification (Passport, Driving License, Voter ID, PAN Card, Aadhaar Card, NREGA Job Card, etc.).
- Politically Exposed Person (PEP): Individuals who are or have been entrusted with prominent public functions by a *foreign country*, including Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, and important political party officials, as well as their family members and close associates.
- High-Risk Customer: A customer or transaction assessed by the NBFC as posing a higher risk of money laundering or terrorist financing based on the NBFC's risk assessment framework.
- Enhanced Due Diligence (EDD): Additional and more stringent CDD measures applied to high-risk customers or situations.
- Simplified Due Diligence (SDD): Reduced CDD measures applied to customers assessed as posing a low risk, where permitted by RBI guidelines.
- Suspicious Transaction Report (STR): A report submitted to FIU-IND regarding transactions or activities suspected to be involved in money laundering or terrorist financing.
- Principal Officer (PO): An officer designated by the NBFC at a management level, responsible for ensuring overall compliance with PMLA obligations and reporting information to FIU-IND.
- Designated Director: A director designated by the NBFC's Board to ensure overall compliance with obligations under PMLA and Rules.
- Central KYC Records Registry (CKYCR): A centralized repository for KYC records of customers in the financial sector, managed by CERSAI.
- Video-based Customer Identification Process (V-CIP): A method of customer identification using live audio-visual interaction, as permitted by RBI for certain categories of customers.
- Unique Customer Identification Code (UCIC): A unique customer ID generated by the NBFC for each customer, to avoid redundant KYC checks for customers seeking additional services.

4. KYC Policy Elements

This KYC Policy incorporates the following four key elements:

1. Customer Acceptance Policy (CAP)

2. Customer Identification Procedures (CIP)
3. Monitoring of Transactions / Ongoing Due Diligence
4. Risk Management

5. Customer Acceptance Policy (CAP)

PCPL shall adhere to a strict Customer Acceptance Policy to ensure that services are not provided to individuals or entities that pose unacceptable ML/TF risks.

5.1. General Guidelines

- No Anonymous/Fictitious Accounts: No account-based relationship shall be opened in anonymous or fictitious/benami names.
- Unable to Conduct CDD: PCPL shall not open any account or continue any business relationship where it is unable to apply appropriate CDD measures, either due to non-cooperation from the customer or non-reliability of the documents/information provided. In such cases, the reasons for inability to complete CDD shall be documented, and a Suspicious Transaction Report (STR) shall be considered.
- Sanctions Screening: Before establishing a relationship or conducting transactions, customers and beneficial owners will be screened against relevant national and international sanctions lists (e.g., UN Security Council Sanctions List, lists issued under UAPA 1967). No relationships will be established with individuals/entities on these lists.
- Customer Presence: While physical presence is preferred, non-face-to-face (NF2F) relationships may be established using permitted methods like V-CIP, Aadhaar OTP-based e-KYC, CKYCR, Digi Locker, etc., with appropriate risk mitigation measures.
- Customer Information: Information sought from the customer shall be relevant to the perceived risk, not intrusive, and in conformity with RBI guidelines. Any other information should be sought separately with the customer's consent.

5.2. Specific Customer Categories

5.2.1. Individuals

- Full legal name, address, date of birth, nationality, PAN/Form 60.
- Purpose of relationship and estimated transaction activity.
- Photograph and signature.

5.2.2. Sole Proprietorship Firms

- Proof of identity and address of the proprietor.
- Proof of existence/activity of the firm (e.g., registration certificate, shop and establishment certificate, GST registration, utility bills in the name of the firm).
- PAN of the proprietor.

5.2.3. Legal Entities (Companies, Partnership Firms, Trusts, Unincorporated Associations/Body of Individuals)

- For the Entity: Legal name, registered address, principal place of business, PAN, nature of business, purpose of relationship, etc. (Refer to RBI Master Direction for specific documents like Certificate of Incorporation, Memorandum & Articles of Association, Partnership Deed, Trust Deed, Resolution of Board/Governing Body).
- For Key Individuals related to the Entity: Identity and address verification (using OVDs) of:
    - Directors, Partners, Trustees, Office bearers/authorized signatories.
    - Beneficial Owner(s) (BOs):
        - Company: Natural person(s) who holds more than 10% of shares or voting rights, or exercises control through other means. If no such person, then the senior managing official.
        - Partnership Firm/Unincorporated Association/Body of Individuals: Natural person(s) who holds more than 15% of capital or profits, or exercises control through other means. If no such person, then the senior managing official.
        - Trust: Author of the trust, the trustee, the beneficiaries, and any other person exercising ultimate effective control over the trust. Where the beneficiary is a juridical person, the BO of the beneficiary also needs to be identified.
- Source of Funds/Wealth: For entities, especially high-risk ones, information on the source of funds/wealth of the entity must be obtained.

6. Customer Identification Procedures (CIP)

The Customer Identification Procedure involves identifying the customer, verifying their identity using reliable, independent source documents, and identifying beneficial owners.

6.1. Verification of Identity and Address

- Officially Valid Documents (OVDs): OVDs (physical or equivalent e-documents thereof) shall be the primary basis for identity and address verification. The list of accepted OVDs is as per the latest RBI Master Direction on KYC (typically Annex I of the MD).
    - For Proof of Identity: Passport, Driving License, Voter's Identity Card, PAN Card, Aadhaar Card (physical or e-Aadhaar), NREGA Job Card, Letter issued by the National Population Register.
    - For Proof of Address: If OVD for identity does not contain current address, then: Utility bill (not more than 2 months old), property/municipal tax receipt, pension/family pension payment orders, letter of allotment of accommodation from employer, documents issued by foreign governments/embassies.
- Self-Declaration for Address Change: If the current address is different from that on the OVD, a self-declaration of the current address may be obtained. A separate proof of address for the declared address must be submitted within 3 months.
- Digital KYC/V-CIP:

- V-CIP:PCPL will utilize V-CIP for onboarding new individual customers, proprietors of proprietorship firms, authorized signatories, and beneficial owners of Legal Entity customers, as per RBI guidelines. This involves a live, consent-based, geotagged, audio-visual interaction, verification of OVDs, liveness detection, and integration with digital verification systems (e.g., Aadhaar e-KYC, Digi Locker, PAN verification).
- Aadhaar OTP-based e-KYC: Used for non-face-to-face onboarding of individual customers, subject to RBI guidelines. Limited accounts opened this way must be converted to full KYC within one year, failing which the account will be closed/frozen.
- CKYCR: Fetching customer KYC records from CKYCR using the CKYC Identifier is a primary mode of identification. When a CKYC Identifier is provided, fresh OVDs are generally not required, subject to verification of identity and an "in-person" liveness check.

6.2. Unique Customer Identification Code (UCIC)

- A unique UCIC will be allotted to each customer to avoid multiple KYC records for the same customer within the NBFC system and to facilitate ease of retrieval.

7. Monitoring of Transactions / Ongoing Due Diligence

PCPL shall exercise continuous vigilance over the business relationships established with customers to ensure that transactions are consistent with the NBFC's knowledge of the customer, their business, risk profile, and, where necessary, the source of funds.

7.1. Account & Transaction Monitoring

- System-Based Monitoring: Implement automated or manual systems to monitor transactions for any unusual patterns or deviations from the customer's expected profile.
- Alert Generation: Systems will generate alerts for transactions that trigger pre-defined thresholds or criteria (e.g., large cash transactions, frequent foreign remittances, transactions with high-risk countries).
- Investigation of Alerts: All alerts shall be promptly investigated by trained personnel. Documentation of investigations and decisions must be maintained.
- Red Flags: Staff must be trained to identify and report red flags (refer to Section 13).

7.2. Periodic Updation of KYC (Re-KYC)

- Customer KYC records, including identity, address, and risk categorization, shall be periodically updated based on the risk category:
  - High Risk Customers: At least once every two years.
  - Medium Risk Customers: At least once every five years.
  - Low Risk Customers: At least once every ten years.

8. Risk Management

PCPL shall adopt a risk-based approach (RBA) to KYC, ensuring that the intensity of CDD measures is proportionate to the assessed money laundering and terrorist financing risks.

8.1. Customer Risk Categorization

- Customers shall be categorized into Low, Medium, or High risk based on a comprehensive assessment of various factors, including:
    - Customer Type: Individuals (salaried, self-employed), Corporate entities (public/private), Partnership firms, HUFs, Trusts, Unincorporated Associations, Sole Proprietorships, PEPs, Non-profit Organizations (NPOs), Entities with complex structures.
    - Geographical Risk: Countries/jurisdictions identified as high-risk by FATF, OFAC, UN Sanctions list, or those lacking robust AML/CFT regimes.
    - Product/Service Risk: Products/services that are inherently higher risk (e.g., high-value loans, gold loans, cash-intensive services, digital lending with non-face-to-face onboarding without robust V-CIP).
    - Delivery Channel Risk: Non-face-to-face relationships, particularly without a robust V-CIP.
    - Behavioral Risk: Unusual or complex transaction patterns, adverse media.
    - Source of Funds/Wealth: Legitimacy and clarity of the source.
- The Board or a Committee of the Board shall determine the periodicity of ML/TF risk assessment review.

8.2. Simplified Due Diligence (SDD)

- SDD may be applied only to demonstrably low-risk customers, as explicitly permitted by RBI guidelines.
- Criteria for SDD: [List specific, RBI-approved low-risk scenarios, e.g., small value loans (if applicable as per RBI), certain government entities, highly regulated entities, etc.].
- Measures under SDD: Reduced frequency of periodic updates, relaxed proof of address for temporary changes (if permitted), reduced intensity of ongoing monitoring. Note: SDD does not exempt the NBFC from collecting PAN/Form 60, photograph, and conducting name screening.

8.3. Enhanced Due Diligence (EDD)

- EDD shall be mandatorily applied to customers or situations identified as high-risk.
- Triggers for EDD:
    - Politically Exposed Persons (PEPs): For foreign PEPs, in addition to standard CDD, EDD measures will include:
        - Obtaining senior management approval to establish/continue the business relationship.
        - Establishing the source of wealth and source of funds.

    - Conducting enhanced ongoing monitoring of the business relationship.
  - Customers from high-risk countries or non-cooperative jurisdictions.
  - Non-profit organizations (NPOs)/NGOs (due to potential for TF abuse).
  - Customers involved in cash-intensive businesses.
  - Customers with complex, opaque, or unusual ownership structures.
  - Transactions that are complex, unusually large, or have no apparent economic/lawful purpose.
  - Customers about whom adverse media is found.
  - Non-face-to-face relationships without robust mitigating controls.
  - Customers where the source of funds/wealth is unclear or suspicious.
- Measures under EDD:
  - Obtain additional information on the customer's source of wealth and source of funds/income.
  - Obtain additional information on the purpose of the business relationship.
  - Obtain senior management approval for establishing/continuing the relationship.
  - Increased frequency and intensity of ongoing monitoring and reviews.
  - More extensive background checks and adverse media screening from reliable independent sources.
  - Physical verification of customer's business/residential premises where deemed necessary (especially for high-value loans or high-risk profiles).

9. Central KYC Records Registry (CKYCR) Compliance

PCPL shall strictly comply with CKYCR requirements:

- Mandatory Upload: Upload KYC records of all new individual accounts opened to CKYCR in the prescribed format.
- CKYC Identifier: Communicate the generated CKYC Identifier to the customer, If Requested by the Customer.
- Fetching Records: Fetch KYC records from CKYCR when a customer submits a CKYC Identifier.
- Updation: Update CKYCR records whenever there is a change in the customer's KYC information or during periodic reviews.
- Verification: Verify the fetched CKYC records for completeness and authenticity. If the record is incomplete or not as per current KYC norms, complete CDD must be performed.

10. Record Keeping

All records pertaining to customer identification, verification, risk assessment, transaction monitoring, STRs, and communications related to KYC shall be maintained diligently.

- Retention Period: All CDD records and transaction records shall be preserved for a minimum period of five (5) years after the business relationship is terminated or after the completion of the transaction (for occasional transactions), as required by PMLA and RBI guidelines.

- Accessibility: Records must be easily retrievable in both physical and electronic formats to facilitate audits and regulatory inspections by RBI, FIU-IND, or other competent authorities.
- Confidentiality: All customer information must be kept confidential and accessed only by authorized personnel.

11. Reporting Suspicious Transactions (STRs)

- Internal Reporting: Any employee who suspects money laundering or terrorist financing activity (based on CDD information, ongoing monitoring, or any other source) must immediately report their suspicion to the Principal Officer (PO).
- Reporting to FIU-IND: The Principal Officer, after due diligence and examination of the suspicion, shall file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit - India (FIU-IND) within the stipulated timeframe (as per PMLA Rules).
- Inability to Apply CDD: If the NBFC is unable to apply appropriate CDD measures for a customer (due to non-cooperation or non-reliability of documents/information), it must consider filing an STR with FIU-IND and take prompt, diligent action, including exiting the relationship if necessary.
- No Tipping-Off: Under no circumstances shall any employee "tip-off" a customer (or any other person) that a report has been or may be filed with FIU-IND. This is a criminal offense under PMLA.
- Confidentiality: The fact that an STR has been filed must be kept strictly confidential.

12. Roles and Responsibilities

- Board of Directors/Senior Management: Overall responsibility for ensuring compliance with AML/CFT laws, PMLA, and RBI guidelines; approving the KYC Policy; and reviewing its effectiveness periodically. The Board or a committee of the Board shall determine the periodicity of ML/TF risk assessment.
- Principal Officer (PO): Oversees the implementation of the KYC policy, acts as the single point of contact with FIU-IND, and is responsible for furnishing STRs/CTRs/NTRs/CCRs to FIU-IND. The PO shall be at a managerial level in the organization's hierarchy.
- Compliance Department/AML Officer: Develops, implements, and maintains the KYC policy; provides guidance and training; conducts internal reviews; and assists the PO.
- Front-Line Staff/Customer-Facing Units: Primary responsibility for conducting initial CDD, collecting KYC documents, verifying information, identifying red flags, and escalating suspicions to the PO/Compliance.
- Operations/Back Office: Responsible for data accuracy, CKYCR uploads/downloads, record keeping, and ensuring proper maintenance of KYC records.
- Internal Audit: Independent assessment of the effectiveness of KYC policies and procedures, adherence to regulations, and reporting findings to the Audit Committee/Board.

13. Red Flags / Warning Indicators

Staff must be trained to identify and escalate potential red flags during the customer onboarding and ongoing monitoring processes. These indicators may warrant further investigation or escalation to the Principal Officer:

- Customer reluctance or refusal to provide complete, accurate, or consistent information/documents.
- Providing suspicious, forged, or altered identification documents.
- Inconsistent or illogical information provided (e.g., business type does not match stated income/transaction patterns).
- Multiple accounts opened by the same individual or entity for no apparent legitimate reason.
- Unusual or inexplicable transactions for the customer's declared business or personal profile.
- Frequent large cash transactions or deposits where the customer's business does not typically involve cash.
- Rapid movement of funds between multiple accounts or different entities.
- Customer from or conducting transactions with high-risk jurisdictions, especially those identified by FATF or subject to sanctions.
- Unexplained wealth or sudden significant increase in transaction volume/value.
- Customer requesting unusually complex or opaque product structures with no apparent economic rationale.
- Use of shell companies or complex layering of legal entities without clear business purpose.
- Adverse media reports concerning the customer or related parties regarding financial crime, corruption, or terrorism.
- Any attempt to structure transactions to avoid reporting thresholds.
- Early repayment of loans without logical explanation, especially for large amounts.
- Frequent changes in beneficial ownership or company structure without valid business reasons.

14. Training

All relevant employees, particularly those in customer-facing roles, compliance, operations, and senior management, shall receive mandatory and ongoing training. This includes:

- Detailed understanding of PMLA, PMLA Rules, and all applicable RBI KYC/AML/CFT guidelines.
- PCPL's internal KYC Policy and procedures, including specific responsibilities.
- Identification of red flags and warning indicators of suspicious activities.
- The internal process for reporting suspicious transactions to the Principal Officer.
- Updates on changes in regulatory requirements or internal policies.

15. Compliance Monitoring and Internal Audit

- The Compliance Department will regularly monitor the implementation and effectiveness of this KYC Policy to ensure adherence to regulatory requirements and internal policies.

- Internal reviews and audits of KYC/AML processes will be conducted periodically to identify any weaknesses or areas for improvement.
- The Internal Audit function shall conduct an independent assessment of the KYC/AML framework, including CDD procedures, at least annually. Audit reports and corrective actions taken must be documented and reported to the Audit Committee and the Board.
- Robust Management Information Systems (MIS) will be maintained to track KYC compliance status, risk profiles, transaction monitoring alerts, and reporting.

List of Officially Valid Documents (OVDs) and other acceptable documents (as per RBI).

Address Proof	Pan and Recent Adhar Card is mandatorily collected. For current address Any one of the following documents can be collected of the respective Hirer, Co-borrower & Guarantor if any. And All the KYC verified as EKYC Individuals: Valid Passport Voter identity card Valid driving license Ration card Registered property documents Latest Property tax receipt (not more than 3 months old) Latest Telephone bill – landline/postpaid (not more than 1 months old) Latest utility bill (not more than 1 month old) including electricity bill, gas bill or new gas card. Others: (Non individuals) Shops and establishment certificate GST registration certificate Registered lease deed Latest property tax bills (Not more than 3 months old) Latest telephone bills (Not more than 1 months old) Latest utility bills. (Not more than 1 months old)

Identity Proof	Any one of the following document can be collected as identity proof for Hirer, Co borrower/ Guarantor/ witness if any- Recent UID (Aadhar) – Unique Identity card Valid Passport Voter identity card Valid PAN card Valid driving license Employee photo ID card issued by Govt Registered property documents with photograph Others: (Non individual) Certification of incorporation or other incorporation documents Valid PAN card Board Resolution shop & establishment Act certificate GST /Sales tax registration certificate MOA/AOA with registration certificate Registered partnership deed.
Signature Verification	The Borrower's signature should be matched with Bank and our agreement, The signature on any of the following documents can be accepted as a valid signature proof PAN Card Driving License Passport Certification / Attestation by bank Government issued ID card with signature

Customer Risk Categorization

Customers are categorized into:

- **Low Risk** (e.g., salaried individuals with steady income)
- **Medium Risk** Self-employed individuals, Small and Medium Enterprises, Foreign nationals or NRIs (with proper documentation) Trusts, NGOs, and charitable organizations
- **High Risk** (e.g., non-resident individuals, high-net-worth customers, politically exposed persons - PEPs)

Periodic review of KYC documents based on risk profile:

- **Low risk** – once every 10 years
- **Medium risk** – once every 8 years
- **High risk** – once every 2 years