

# KYC & AML Policy

Dhruva Capital Services Limited (NBFC)

---

## 1. Introduction

This KYC & AML Policy (“Policy”) is adopted by **Dhruva Capital Services Limited** (“Company”), a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India.

The Company offers digital lending services through its platform **NeoMoney** (mobile application and website).

### **Regulatory Disclosure:**

All loans are **sanctioned and disbursed solely by Dhruva Capital Services Limited**. NeoMoney acts only as a **digital platform facilitating customer onboarding and servicing**.

This Policy is framed in compliance with:

- RBI Master Direction – Know Your Customer (KYC)
  - Prevention of Money Laundering Act, 2002 (PMLA)
  - Digital Lending Guidelines (RBI)
  - Applicable rules, notifications, and circulars
- 

## 2. Objective

The objectives of this Policy are to:

- Prevent money laundering, terrorist financing, and fraud
  - Ensure proper customer identification and verification
  - Establish a risk-based approach to customer onboarding
  - Ensure compliance with regulatory obligations
  - Protect the integrity of the financial system
-

### 3. Scope

This Policy applies to:

- All customers/borrowers of the Company
  - Digital onboarding via NeoMoney platform
  - All employees, agents, and authorized service providers
  - Third-party service providers involved in onboarding or verification
- 

### 4. Definitions

- **KYC (Know Your Customer):** Process of verifying customer identity
  - **AML (Anti-Money Laundering):** Measures to prevent illegal financial activities
  - **Customer:** Any individual applying for or availing financial services
  - **Officially Valid Documents (OVDs):** As defined by RBI (e.g., Aadhaar, PAN, Passport, Voter ID, Driving License)
- 

### 5. Customer Acceptance Policy (CAP)

The Company shall:

- Not open anonymous or fictitious accounts
- Accept customers only after proper KYC verification
- Reject onboarding where identity cannot be verified
- Apply enhanced due diligence for high-risk customers

The Company reserves the right to decline applications without assigning reasons where risk is unacceptable.

---

### 6. Customer Identification Procedures (CIP)

Customer identification shall be carried out using:

#### 6.1 Officially Valid Documents (OVDs)

- Aadhaar (subject to consent and applicable regulations)
- PAN (mandatory for financial transactions)
- Passport / Voter ID / Driving License

## 6.2 Digital KYC Methods

- Aadhaar-based e-KYC (where permitted)
- Video KYC (V-CIP) as per RBI guidelines
- OTP-based authentication
- CKYC registry verification

## 6.3 Additional Verification

- Mobile number verification (OTP)
  - Bank account validation
  - Facial recognition / liveness detection (where applicable)
- 

# 7. Customer Due Diligence (CDD)

The Company follows a **risk-based approach**:

## 7.1 Risk Categorization

Customers are classified as:

- Low Risk
- Medium Risk
- High Risk

Based on:

- Occupation
  - Income profile
  - Geographic location
  - Transaction behavior
  - Credit history
- 

## 7.2 Enhanced Due Diligence (EDD)

For high-risk customers:

- Additional documentation may be required
  - Source of funds verification
  - Continuous monitoring of transactions
- 

# 8. Politically Exposed Persons (PEPs)

- PEPs shall be identified at onboarding stage
  - Senior management approval is required before onboarding
  - Enhanced monitoring shall be applied
- 

## 9. Ongoing Monitoring of Transactions

The Company shall:

- Monitor transactions for unusual or suspicious patterns
- Identify deviations from normal customer behavior
- Flag high-value or abnormal transactions

Automated systems may be used for monitoring and alerts.

---

## 10. Suspicious Transaction Reporting (STR)

In case of suspicious activity:

- The Company shall report to the **Financial Intelligence Unit – India (FIU-IND)**
  - Reports shall be filed within prescribed timelines
  - Confidentiality of reporting shall be maintained
- 

## 11. Record Keeping

The Company shall maintain:

- KYC records and identity documents
- Transaction records
- Account files and correspondence

Retention period:

- Minimum **5 years** after end of relationship (as per PMLA/RBI guidelines)
- 

## 12. Data Privacy & Security

Customer data shall be:

- Collected with explicit consent
- Stored securely with encryption
- Used only for lawful purposes

The Company complies with:

- RBI data localization requirements
  - Applicable data protection laws
- 

## 13. Third-Party Reliance

Where third-party service providers (LSPs) are used:

- The Company remains fully responsible for KYC compliance
  - Due diligence shall be conducted on such providers
  - Data sharing shall be secure and consent-based
- 

## 14. Employee Training & Compliance

- Employees shall undergo regular AML/KYC training
  - Staff shall be aware of regulatory requirements and red flags
  - Internal audits shall be conducted periodically
- 

## 15. Internal Controls & Audit

The Company shall maintain:

- Robust internal control systems
  - Independent audit of KYC/AML processes
  - Periodic compliance reviews
- 

## 16. Grievance Redressal

For KYC-related concerns:

**Dhruva Capital Services Limited**

Grievance Redressal Officer: Ramesh Kumar Pandey

Email: [grievance@dhruvacapital.com](mailto:grievance@dhruvacapital.com)

**NeoMoney Platform (Service-related issues):**

Bishwajit Ghosh

Email: [grievance@neomoney.app](mailto:grievance@neomoney.app)

Unresolved complaints may be escalated to:

RBI Integrated Ombudsman Scheme

Website: <https://cms.rbi.org.in>

Toll-Free: 14448

---

## **17. Policy Review & Updates**

- This Policy shall be reviewed annually
  - Updates shall be made based on regulatory changes
  - Latest version will be published on:
    - <https://www.dhruvacapital.com/>
    - <https://neomoney.app/>
- 

## **18. Public Disclosure**

This Policy is available on the Company's website in compliance with RBI requirements.