KYC & Anti-Money Laundering (AML) Policy

1. Introduction

Barota Finance Limited, through its digital lending platform **Paisa24Finance**, is committed to maintaining robust Know Your Customer (KYC), Customer Due Diligence (CDD) and Anti-Money Laundering (AML) practices.

The Company seeks to prevent its products and services from being misused for money laundering, terrorist financing, fraud or other unlawful activities. This Policy establishes the broad principles and controls adopted by the Company for customer identification, verification, monitoring, risk assessment, record keeping and reporting, in accordance with applicable laws and regulatory requirements.

2. Objectives

- Establish appropriate customer identification and verification procedures.
- Prevent misuse of the Company's products and services for money laundering, terrorist financing, fraud or other unlawful activities.
- Assess and manage customer and relationship-level AML/KYC risks.
- Maintain appropriate monitoring, record-keeping and reporting mechanisms.
- Protect customer information and maintain confidentiality.
- Ensure compliance with applicable KYC, AML and regulatory requirements.
- Promote awareness and accountability among relevant employees and service providers.

3. Regulatory Framework

The Company shall maintain its KYC and AML framework in accordance with applicable laws, rules, regulations and regulatory directions governing its activities, including applicable requirements issued by the Reserve Bank of India (RBI), the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money Laundering (Maintenance of Records) Rules, applicable KYC Directions and other applicable legal or regulatory requirements.

Where regulatory requirements change, the Company may update its policies, procedures and controls accordingly.

4. Customer Identification and KYC

The Company shall undertake appropriate customer identification and verification before establishing a customer relationship or providing financial services, as applicable.

KYC information and documents may include identity, address, contact, financial and other information required under applicable law and regulatory requirements.

The Company may use legally permitted digital KYC, electronic verification, document verification and other approved methods for customer identification and verification.

5. Customer Due Diligence (CDD)

The Company shall conduct appropriate Customer Due Diligence based on the nature and risk of the customer and the relevant financial activity.

CDD may include identification and verification of the customer, understanding the purpose and nature of the relationship, assessing relevant risk factors and obtaining additional information where required.

The Company may decline, restrict or discontinue a relationship where required KYC information cannot be satisfactorily obtained or verified, subject to applicable law and internal procedures.

6. Beneficial Ownership

Where applicable, the Company shall take reasonable and legally required steps to identify and verify the beneficial owner of a customer or entity.

Beneficial ownership information shall be assessed in accordance with applicable legal and regulatory requirements and maintained as required.

7. Customer Risk Categorisation

The Company may classify customers into appropriate risk categories based on relevant factors such as customer profile, product or service, transaction or repayment behaviour, geography, delivery channel and other risk indicators.

Enhanced due diligence and additional controls may be applied to customers or relationships presenting higher risks, as required by applicable law and the Company's internal procedures.

8. Enhanced Due Diligence

Where higher risk is identified, the Company may undertake enhanced due diligence, including obtaining additional information, carrying out additional verification, applying enhanced monitoring or obtaining appropriate management approval, as applicable.

The extent of enhanced due diligence shall be proportionate to the identified risk and consistent with applicable regulatory requirements.

9. Politically Exposed Persons (PEPs)

The Company shall maintain appropriate procedures for identifying and handling customers or beneficial owners who fall within the applicable definition of Politically Exposed Persons (PEPs).

Where required, enhanced due diligence, appropriate approval and enhanced monitoring may be applied in accordance with applicable regulatory requirements.

10. Sanctions and Screening

The Company may conduct screening of customers and relevant parties against applicable sanctions lists, watchlists and other legally recognised sources, as required.

Potential matches shall be reviewed and handled in accordance with applicable legal, regulatory and internal procedures.

11. Transaction and Activity Monitoring

The Company maintains appropriate mechanisms for monitoring customer activities, transactions and repayment-related activity for unusual, suspicious or potentially unlawful patterns.

Monitoring may consider customer profile, transaction behaviour, frequency, amount, unusual activity, inconsistencies in information and other relevant risk indicators.

Where suspicious activity is identified, it shall be reviewed and escalated in accordance with applicable internal procedures and legal or regulatory reporting requirements.

12. Suspicious Transaction Reporting

Where required by applicable law, the Company shall report suspicious transactions or other reportable matters to the appropriate authority, including the Financial Intelligence Unit – India (FIU-IND), in accordance with applicable requirements.

The Company shall maintain appropriate procedures for investigation, escalation, documentation and regulatory reporting of suspicious activities.

13. Record Keeping

The Company shall maintain KYC records, customer identification information, transaction-related records and other records required under applicable laws and regulations for the prescribed period.

Records shall be maintained in a manner that enables appropriate retrieval and production to competent authorities when legally required.

14. Data Protection and Confidentiality

KYC and AML information may contain sensitive customer and financial information. The Company shall maintain appropriate safeguards to protect such information against unauthorised access, misuse, disclosure, alteration or loss.

Customer information shall be handled in accordance with applicable privacy and data-protection requirements and the Company's Privacy Policy.

Information may be disclosed to regulators, law-enforcement authorities or other authorised parties where required or permitted by law.

15. Prohibition of Anonymous or Fictitious Accounts

The Company shall not knowingly establish or maintain anonymous, fictitious or improperly identified customer relationships where prohibited by applicable law or regulatory requirements.

16. Reliance on Third Parties and Service Providers

Where permitted by applicable law and regulatory requirements, the Company may use authorised service providers or regulated partners for certain KYC, verification, technology or operational activities.

The Company shall maintain appropriate oversight, contractual controls and monitoring mechanisms to manage risks arising from such arrangements.

17. Employee Awareness and Training

Employees and relevant personnel involved in customer onboarding, credit, operations, compliance, technology, risk management and customer servicing shall receive appropriate awareness or training regarding KYC, AML, fraud prevention and applicable regulatory requirements.

18. Compliance and Governance

The Company shall maintain appropriate governance, oversight and accountability for implementation of its KYC and AML framework.

Material KYC or AML concerns may be escalated to the appropriate compliance, risk management or senior management authority in accordance with internal procedures.

19. Internal Controls and Audit

The effectiveness of KYC and AML controls may be reviewed through internal monitoring, compliance reviews, audits, testing and other appropriate assurance mechanisms.

Identified deficiencies may be addressed through corrective and preventive actions, process improvements, additional controls or employee training.

20. Policy Review

This Policy shall be reviewed periodically and whenever there are significant changes in applicable laws, regulations, RBI directions, products, technology, business activities or the Company's risk profile.

The Company may amend or update this Policy to maintain alignment with applicable requirements.

21. Compliance with Applicable Law

In the event of any conflict between this Policy and any applicable law, regulation or regulatory direction, the applicable law, regulation or regulatory direction shall prevail.

22. Contact Information

For any queries relating to this KYC & Anti-Money Laundering Policy, customers and other stakeholders may contact:

Barota Finance Limited
Through Paisa24Finance

Email: care@paisa24finance.com
Website: Paisa24Finance.com
Contact No.: +91 98881 33360

RBI Registration No.: B-06.00606

This KYC & Anti-Money Laundering Policy is subject to applicable laws, regulations and regulatory directions and may be updated from time to time.