NJT FINANCE®
We value your needs.

KNOW YOUR CUSTOMER & ANTI-MONEY LAUNDERING POLICY

NJT FINANCE PRIVATE LIMITED

Registered Office: Old No. XII/0235 C1 & C2, New No. II/1007 C1& C2
TRINITY BUILDING, Kottayam, KOTTAYAM, Kerala, India, 686028
Email ID: abisonjohney@njtfinance.com, Website: www.njtfinance.com
Phone No.: +91-9061755000, +91-97478 55000
CIN: U65910KL1995PTC008909

CONTENTS

INTRODUCTION

NJT Finance Private Limited ("the Company") is committed to maintaining robust Know Your Customer ("KYC") and Anti Money Laundering ("AML") standards to prevent the misuse of its financial services for money laundering, terrorism financing, and other illicit activities. This policy sets out the Company's approach to complying with applicable laws and regulations, including the Prevention of Money Laundering Act, 2002 (PMLA) and RBI Master Directions on KYC, and establishes procedures for customer identification, risk assessment, monitoring, and reporting.

OBJECTIVES

The primary objectives of this policy are to:

- Ensure compliance with applicable KYC and AML laws, regulations, and guidelines.
- Establish a transparent process for identifying and verifying customers.
- Prevent Company's services from being used for money laundering or financing of terrorism.
- Detect and report suspicious activities to the appropriate authorities.
- Protect the Company's reputation and promote ethical conduct.

SCOPE

This policy applies to all products and services offered by the Company, across its head office and any future branches. All employees, agents, contractors, and third-party service providers involved in customer onboarding, transaction processing, or monitoring shall comply with this policy.

DEFINITIONS

Customer: A person or entity engaged in a financial transaction with the Company.

Beneficial Owner (BO): The natural person who ultimately owns or controls a customer, including those with more than 10% ownership or controlling interest.

Politically Exposed Person (PEP): Individuals who are or have been entrusted with prominent public functions, including their immediate family members and close associates.

Suspicious Transaction: A transaction that gives rise to a reasonable ground of suspicion that it may involve proceeds of crime or be related to money laundering or terrorist financing.

ROLES & RESPONSIBILITIES

- Designated Director: A Whole-Time Director or Managing Director appointed by the Board, responsible for overall compliance with KYC/AML obligations.
- Principal Officer: A senior officer nominated by the Board, responsible for monitoring transactions, ensuring compliance, and reporting to FIU-IND.

CUSTOMER ACCEPTANCE POLICY (CAP)

Company shall:

- Not open accounts or conduct transactions in anonymous or fictitious names.
- No introduction from existing customers or third parties shall be required or accepted for opening new accounts.
- Carry out appropriate due diligence before establishing a business relationship. If CDD cannot be completed, the Company shall refuse to open the account and consider filing a Suspicious Transaction Report (STR) where applicable.
- Categorize customers into low, medium, or high-risk profiles, applying enhanced due diligence where necessary.

- Obtain sufficient information to establish the true identity of customers and beneficial owners.

- Avoid unnecessary hurdles that may exclude financially or socially disadvantaged persons from accessing services.

CUSTOMER IDENTIFICATION PROCEDURES (CIP)

- CIP shall be conducted for transactions of INR 50,000 or more involving third-party or in-house products. Procedure shall apply to walk-in customers conducting single or connected transactions of INR 50,000 or above. This requirement shall be triggered if transactions are suspected of being structured to avoid applicable reporting thresholds

- Collect and verify KYC documents such as PAN, Aadhaar, and proof of address as per RBI Master Directions.

- Verify customer identity using reliable, independent sources. Where PAN is collected, it shall be verified using the Income Tax Department's online system. GST registration details shall be verified through the official GST portal. Digital signatures on electronic documents shall be verified through certifying authority portals.

- Obtain additional documents for non-individual customers (e.g., companies, partnerships, trusts) including proof of legal existence and authorization for signatories. CDD shall be individually carried out for each joint account holder

- Where additional information beyond regulatory requirements is collected, explicit consent shall be obtained from the customer.

- Each customer shall be assigned a Unique Customer Identification Code (UCIC) at the time of onboarding, as per RBI guidelines, to ensure proper tracking of the customer's relationship across products and services. Repeat CDD shall not be required for existing KYC-compliant customers identified by their UCIC, except where triggered by risk or regulatory changes.

- Third parties relied upon for CDD must be regulated and supervised and not based in high-risk jurisdictions. The company shall retain responsibility for CDD even when third-party services are used. Customer records shall be immediately retrievable either from the third party or the Central KYC Registry.

- Conduct periodic KYC updates: at least once every 10 years for low-risk, 8 years for medium-risk, and 2 years for high-risk customers.

RISK ASSESSMENT & CATEGORIZATION

Customers will be risk-rated based on factors including type of business, source of funds, geographic location, origin or destination of transactions, transaction volume, and customer profile. Information collected for risk profiling shall be relevant, minimal, and non-intrusive. The company shall consider whether identity documents can be authenticated online through issuing authority portals.

The risk assessment exercise shall be carried out periodically, and the periodicity shall be determined by the Board of Directors in alignment with the outcome of the risk assessment exercise. However, in any case, the risk categorization shall be reviewed at least annually.

Risks associated with delivery channels, including digital onboarding or agent-assisted sourcing, shall be evaluated during risk categorization. Risk categorization will be reviewed at least annually. Company shall refer to guidance from FATF, IBA, RBI, and other competent authorities to update risk assessment practices. Risk classification and its underlying rationale shall remain confidential and not disclosed to customers. Risk categories:

- Low Risk: Customers with strong financial track record, high profitability, stable cash flow, excellent credit history and offer high-quality collateral.

- Medium Risk: Customers with a good operational track record but some financial weaknesses, such as inconsistent profitability or a slightly higher debt level. They may have a good credit history but limited collateral.

- High Risk: Customers new businesses with no credit history, businesses with a history of financial losses, high debt, or poor cash flow. They may also have a weak credit history or insufficient collateral. These customers are either denied a loan or offered it at very high interest rates. Non-residents, PEPs, high-net-worth individuals, real estate developers.

ONGOING MONITORING

The company shall continuously monitor customer transactions to ensure they align with the customer's risk profile and expected transaction patterns. Transactions inconsistent with a customer's known profile or exhibiting unusual complexity shall be subjected to further scrutiny. High-risk customers shall undergo enhanced monitoring, including closer examination of large or complex transactions without apparent economic rationale. The company will maintain complete and accurate records of transactions and customer profiles to support effective monitoring. All customers shall be screened against applicable sanctions lists published by authorities such as the UN, OFAC, EU, and RBI/GOI notifications. CDD should not be conducted in a manner that alerts the customer if suspicion of money laundering or terrorist financing exists.

REPORTING REQUIREMENTS

- Suspicious transactions and cash transactions above regulatory thresholds shall be reported to the Financial Intelligence Unit – India (FIU-IND) in the prescribed format and timeline.

- The Principal Officer shall oversee the filing of Suspicious Transaction Reports (STRs) and ensure timely compliance.

RECORD KEEPING

Customer identification documents and transaction records shall be preserved for at least eight years after the end of the business relationship or transaction date, whichever is later. Records shall be maintained in a manner that allows quick retrieval and inspection by regulators.

EMPLOYEE TRAINING & CUSTOMER AWARENESS

- The Company shall conduct periodic training programs for relevant employees to ensure understanding of KYC/AML requirements and detection of suspicious transactions.
- The Company shall also educate customers on the importance of KYC compliance through brochures, website information, and direct communication.

COMPLIANCE

All employees, agents, and contractors of the Company must fully comply with KYC & AML Policy and applicable laws. Non-compliance will result in disciplinary action, including possible termination or legal proceedings. The Principal Officer shall oversee implementation and reporting. The Company will conduct periodic reviews to ensure ongoing adherence.

REVIEW OF POLICY

This KYC & AML Policy shall be reviewed annually or as required by changes in regulatory requirements, business operations, or risk profile. The Board of Directors shall approve all updates to the policy.

ANNEXURE 1

CUSTOMER IDENTIFICATION REQUIREMENTS

INDIVIDUAL CUSTOMERS

- **Mandatory Documents:**
  PAN Card
  Aadhaar Card (or other officially valid document [OVD] such as Passport, Voter ID, Driving License)
  Proof of Address (if different from Aadhaar): Recent utility bill, bank account statement, or rental agreement.
- **Photograph:** Recent passport-sized color photograph.
- **Verification:** Original documents to be verified in-person or through approved e-KYC mechanisms.

SOLE PROPRIETORSHIP FIRMS

- **Proof of existence:** GST Registration Certificate, Shop & Establishment Certificate, or equivalent municipal registration.
- PAN of the proprietor.
- KYC documents of the proprietor (as per individual requirements).

PARTNERSHIP FIRMS

- Partnership Deed.
- Registration Certificate (if registered).
- PAN of the firm.
- GST certificate
- KYC documents of all partners and authorized signatories.

COMPANIES (PRIVATE/PUBLIC)

- Certificate of Incorporation.
- Memorandum & Articles of Association.
- PAN of the company.
- A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf. KYC documents of directors holding 10% or more shares, and of authorized signatories.

BENEFICIAL OWNERSHIP

- Identification and verification of beneficial owners holding 10% or more shares/control for companies and other legal entities.