MITRATA

Mitrata Inclusive Financial Services Pvt. Ltd.

Know Your Customer & Anti-Money Laundering Policy

SCOPE

Applicability

This "Know Your Customer and Anti-Money Laundering Policy" (**the Policy**) will apply to **Mitrata Inclusive Financial Services Private Limited** (hereinafter referred to as '**the Company**'), its employees and its agents/representatives.

This Policy will require the Company's employees and its agents/ representatives to:

- Protect the Company from being used for any type of money laundering or terrorist fundingactivities;
- Comply with the applicable Anti-Money Laundering (AML) Laws and the Company's KYC & AML Policy & Procedures in letter and spirit;
- Be alert and escalate suspicious activity and not knowingly provide advice or other assistance to individuals who attempt to violate Anti Money Laundering Laws or this Policy. Knowledge includes the concept of 'willful blindness' (failure to make appropriate inquiries when faced with suspicion of wrongdoing) and 'conscious avoidance of knowledge';
- Conduct themselves in accordance with the highest ethical standards; and
- Co-operate with the regulatory authorities and the Financial Intelligence Unit as per the applicablelaws.

EffectiveDate

This Policy shall be effective from the date of approval of this policy

Review ofPolicy

The Policy shall be reviewed as and when required by the applicable rules and regulations.

PolicyApproval

The Policy and any significant changes therein shall be approved by the Board of Directors of the Company.

BACKGROUND

The term 'Money Laundering' refers to act of concealing or disguising origin and ownership of proceeds from criminal activities including drug trafficking, public corruption, terrorism,fraud, human trafficking and organized crime activities. 'Terrorist Financing' is the use of legally or illegally obtained funds to facilitate terrorist activities. 'Money Laundering' and 'Terrorist Financing' may involve a wide variety of financial products, services and transactions including lending & investment products, financing of equipment or other property that could be used to facilitate terrorism and other criminal activity.

Almost every crime with a profit motive can create proceeds that can be laundered. For example, fraud, theft, illegal drug sales, organized crime, bribery, corruption of government officials and human trafficking can create illegal funds that a criminal seeks to convert into legitimate property without raising suspicion. Tax evasion and violations of fiscal laws can also lead to money

laundering.

Generally, the process of Money Laundering involves three stages, viz. (i) Placement; (ii) Layering; and (iii) Integration. As illegal funds move from the placement stage to the integration stage, it becomes increasingly harder to detect and trace back to the illegal source.

- **Placement** is the point where illegal funds first enter the financial system. The deposit of illegal cash into an account or the purchase of money orders, cashier's checks or other financial product is made. Non-bank financial institutions, such as currency exchanges, money remitters, casinos, and check-cashing services can also be used for placement.
- **Layering** After illegal funds have entered the financial system, layers are created by closing and opening accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.
- **Integration** occurs when the criminal believes that there are sufficient number of layers hiding the origin of the illegal funds to safely invest the funds or apply them towards purchasing valuable property in the legitimate economy.

A financial institution or other business may be used at any point in the process of money laundering. The criminals and other anti-social elements keep coming-up with innovative means to launder money and no financial institution or business is immune from possible victimization.

To address issue of money laundering, the Government of India and other countries around the world have made money laundering a crime and prescribed regulatory requirements for compliance by the banks, financial companies/ institutions and other regulated/ reporting entities to prevent and detect money laundering.

To prevent money-laundering in India and to provide for confiscation of property derived from or involved in money-laundering and related matters, the Government of India enactedthePreventionofMoneyLaunderingAct,2002(**PMLA**),as amended from time to time. Further, the PMLA and necessary Notifications/ Rules there under have been published and amended thereafter.

As per the Prevention of Money Laundering Act 2002, **"Offence of Money Laundering"** is defined as *"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering.*

Further, **"Proceeds of crime"** *means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."*

The PMLA and the Rules notified there under impose obligation on banking companies, financial institutions (which includes chit fund Company, a co-operative bank, a non- banking financial company and a housing finance institution) and other defined intermediaries to verify identity of clients, maintain records and furnish requisite information to Financial Intelligence Unit- India (FIU-IND). The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

The KYC and AML Policy has been prepared considering the following key elements:

a) To lay down the criteria for Customer Acceptance(CAP);

b) Risk Management;

c) To lay down criteria for Customer Identification Procedures(CIP);

d) To establish procedures for monitoring of transactions as may be applicable;

2. DEFINITIONS

For this Policy, definition of various terms used is as under:

Cash Transaction Report (CTR)- CTR will include the following:

a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency.

Central KYC Records Registry (CKYCR) means an entity defined under Rule 2(1)(aa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

Counterfeit Currency Transaction- All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine. These cash transactions should also include transactions where forgery of valuable security or documents has taken place.

Customer- For the purpose of KYC Norms, a 'Customer' is defined as a person who is engagedinafinancialtransactionoractivitywithareportingentityandincludesaperson on whose behalf the person who is engaged in the transaction or activity, is acting.

Customer Due Diligence (CDD)- Identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'Proof of Identity' and a 'Proof ofAddress'.

Designated Director- means a person designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the Rules thereunder andincludes:-

a) the Managing Director or a whole-time Director duly authorized by the Board of Directors,

b) A person of senior management official designated by the Company as "Designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act,2012.

However, in no case, the Principal Officer should be nominated as the "Designated Director".

KYC Templates means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities, as required by the relevant Rules.

Non-face-to-face customers- Customers who open accounts without visiting the branch/ offices

of the Company or meeting itsofficials.

Officially valid document (OVD)- Any document notified/ advised by the Central Government/ Regulatory Authorities as officially valid document for verifying identity and proof of address ofcustomers.

As on date, OVD means the passport, the Driving License, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, Digital Ration Card, Job Card issued by NREGA duly signed by an officer of the State Government, Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

Explanation: Customers, at their option, shall submit one of the above mentioned OVDs for proof of identity and proof of address.

Further, information provided through prescribed e-KYC process will also be treated as an 'Officially Valid Document' and will be a valid process for KYCverification.

On-going Due Diligence- Regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source offunds.

Periodic Updation means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI, the PMLA and the Rulesthereunder.

Politically Exposed Persons- Individuals who are or have been entrusted with prominent public functions, e.g., Heads of States/Governments, senior politicians, senior government/ judicial/military officers, senior executives of state-owned corporations, important political party officialsetc.

Principal Officer (PO)- An official designated by the Board of Directors of the Company forover seeing and managing the KYC & AML policies and processes. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

'Senior Management' for the purpose of KYC compliance shall include members of the Executive Committee, Designated Director,Principal Officer (PO) and his supervisor.

Suspicious transaction means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime, regardless of the value involved;or

b) appears to be made in circumstances of unusual or unjustified complexity;or

c) appears to have no economic rationale or bona fide purpose;or

d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating toterrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance

terrorism.

Transaction- means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof andincludes:

a) opening of anaccount;

b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physicalmeans;

c) the use of a safety deposit box or any other form of safedeposit;

d) entering into any fiduciaryrelationship;

e) any payment made or received in whole or in part of any contractual or other legalobligation;

f) establishing or creating a legal person or legalarrangement.

Walk-in Customer- means a person who does not have an account based relationship with the Company, but undertakes transactions with theCompany.

CUSTOMER ACCEPTANCE POLICY (CAP)

In accordance with various guidelines issued by RBI on "Know Your Customer Guidelines & Anti Money Laundering Standards" and provisions of the PMLA, the Company has formulated Customer Acceptance Policy (CAP) which lays down the broad criteria for acceptance of customers.

The features of the CAP are detailed below:

a) The Company will follow the Joint Liability Group (JLG) model, where clients are organized into groups and are required to undergo Compulsory Group Training (CGT) and Group Recognition Test (GRT). Under the mentioned processes, the staff verifies client identity by undertaking the necessary KYC documents and verifying with originals. All clients are assessed for the location of residence and business during CGT and GRT.

b) The Company shall ensure that:

i. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.

ii. No transaction is done with an account holder who holds account in an anonymous or fictitious/benami name.

iii. No transaction or account based relationship will be undertaken without following the CDDprocedure.

iv. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation will be specified

v. Optional or additional information will be obtained with an explicit consent of the customer after the account isopened.

vi. The Company will ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. For this purpose, the Company shall maintain lists of individuals or entities

issued by RBI, United Nations Security Council, other regulatory & enforcement agencies, internal lists as the Company may decide from time to time. Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be treated as suspicious andreported.

c) The nature and extent of basic due diligence measures to be conducted at the time of establishment of account opening/ relationship, would depend upon the risk category of the customers and involve collection and recording of information by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the risks posed by the applicant and the applicant's expected use of the Company's products and services from an AML perspective.

d) The information collected from the customer shall be keptconfidential.

e) In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures shall beadopted.

f) Where the Company is unable to apply appropriate KYC measures due to non- furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such adecision.

The aspects mentioned in the CAP would be reckoned while evolving the KYC/AML procedures for various types of customers and products. However, while developing the KYC/CDD procedures, the Company will ensure that its procedures do not become too restrictive or pose significant difficulties in availing its services by deserving general public, especially the financially and socially disadvantaged sections of society.

RISK MANAGEMENT

For Risk Management, the Company shall have a risk based approach which includes thefollowing:

a) Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of theRE;

b) The Company shall exercise proper due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the customers. It shall ensure proper management oversight, systems and controls, segregation of duties, training and other related matters.

c) The customers will be monitored on regular basis with built in mechanism for tracking irregular behavior for risk management and suitable timely corrective action.

CUSTOMER IDENTIFICATION PROCEDURES(CIP)

The Company shall ensure that it will not enter into any transaction with a client where it is unable to identify and obtain required documents. The organization will ensure the identity of the customer and verify the address and other details, thereby protecting the Company against any fraud or misuse. The Company shall collect photocopy of the customer documents after verifying the documents with the original KYC.

Maintenance of Records for Effective KYC/AML Procedure

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act, 2002 and Rules made thereunder. The Company shall:

(a) maintain all necessary records of transactions between the Company and the customer, for at least five years from the date of transaction;

(b) preserve the records pertaining to the identification of the customers and their addresses obtained for at least five years after the business relationship is ended;

(c) make available the identification records and transaction data to the competent authorities upon request;

(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

i. the nature of the transactions;

ii. the date on which the transaction was conducted; and

iii. the parties to the transaction.

Monitoring of Transactions

The Company has established various checks to ensure that identified individuals take the loans. The Field Officer (FO) is required to visit each client's house for evaluation and appraisal of the client and spouse at the time of group formation. The FO needs to ensure the identity and address of the client with the KYC. At the time of CGT, it is ascertained that all the clients are present and know each other. Area Manager or Area Credit Manger undertakes GRT. GRT is conducted with the objective of establishing client identity and ensuring that only identified individuals take the loans and there are no ghost/ dummy clients. Once loans are disbursed to the clients, the Company undertakes Loan Utilization Check (LUC) to ensure the utility and correct usage of the loan provided. The process involves ensuring that agents are not involved who siphon off the money to unspecified purposes. The results of the LUC form an important part of eligibility criteria for future loan cycles.

Internal Audit for Effective KYC/AML Procedure

The Company's internal audit function has a major role in evaluating and ensuring adherence to the KYC/ AML policies and procedures. The internal audit is conducted at Company's branch offices on a regular basis. The internal audit team covers all the branch level processes including documentation, CGT, GRT and collection meetings. The audit team specifically checks Loan documentation to ensure that loans have been provided to clients only after acquiring proper KYC documentation. To ensure that proper client identity is established, the audit team visits a sample of clients either individually or during collection meetings. CGT, GRT and collection meeting process is attended by the audit team to ensure that effective processes are being followed and no agents/ ghosts/ dummy clients exist in the system. Any process related lapses are reported to the branches and senior management for rectification.

List of KYC documents required

As per SRO's KYC Standards, there are FOUR valid documents as under:

1. Voter's Identity Card (Voter ID) issued by the Election Commission

2. Aadhaar card or letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.
3. MNREGA Job card duly signed by an officer of the state government
4. Ration Card issued by the state government of India

What are KYC norms at each client level?

1. At least two (2) KYC documents (from amongst 4 valid documents) has to be captured for every loan given to a borrower . Collection of Voter ID is mandatory for all the states.
2. FO will first enter Aadhar number in Finpage before uploading scan image of Aadhar.
3. While taking photograph of original Aadhaar Card in Finpage, FO must put a paper strip to cover the Aadhaar Number so that only last four digits of Aadhaar ID number are visible.
4. If Aadhaar card number is uploaded with all numbers ACM will immediately notify to FO/BM for necessary correction and get the correct image uploaded.
5. In case Aadhaar ID is not available, branch staff can collect Digital Ration Card, Driving License, Passport, Job Card by MNREGA and PAN Card.

REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA

In accordance with the requirements under PMLA, the Company will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit- India(FIU-IND):

a) **Cash Transaction Report (CTR)-** If any such transactions detected, Cash Transaction Report (CTR) for each month by 15thof the succeeding month.

b) **Counterfeit Currency Report (CCR)-** All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15thof the succeeding month.

c) **Suspicious Transactions Reporting (STR)-** The Company will endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to FIU-IND.

The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed.

SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company will capture the KYC information for sharing with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, under the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company will upload the KYC data pertaining to all types of prescribed accounts with CKYCR, as and when required, in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

INDEPENDENT EVALUTION

To provide reasonable assurance that its KYC and AML procedures are functioning effectively, an audit of its KYC and AML processes will covered under Internal Audit of the Company.

The audit findings and compliance thereof will be put up before the Audit Committee of the Board

on quarterly intervals till closure of audit findings.

RESPONSIBILITIES OF THE SENIORMANAGEMENT

Designated Director- The Company shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules thereunder. The "Designated Director" can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the "Designated Director".

Principal Officer- An official (having knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business) shall be designated as the Principal Officer of the Company. The Principal Officer will responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

Key Responsibilities of the senior management

i) Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under PMLA.

ii) Proper implementation of the company's KYC & AML policy and procedures.

RECORDMANAGEMENT

Record-keeping requirements-The Company shall introduce a system of maintaining proper record of transactions required under PMLA as mentioned below:

a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign

c) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions;

d) all suspicious transactions whether or not made in cash; and

e) records pertaining to identification of the customer and his/her address; and

f) should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

Records to contain the specified information- The records should contain the following information:

a) the nature of the transactions;

b) the amount of the transaction and the currency in which it was denominated;

c) the date on which the transaction was conducted; and

d) the parties to the transaction.

Internal ML/TF risk assessment by the Company

Mitrata has carried out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. While assessing the ML/TF risk, the Company are required to take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time. Further, the internal risk assessment carried out by the Company should be commensurate to its size, geographical presence, complexity of activities/structure, etc.

Further Mitrata has applied the Risk Based Approach (RBA) for mitigation and management of the identified risk.

HIRING OF EMPLOYEES, THEIR TRAINING AND EDUCATION OF CUSTOMERS

Hiring of Employees and Employee training- Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

On-going employee training programme will be put in place so that the members of staff are adequately trained in KYC & AML policy.

Implementation of KYC Procedures requires the Company to seek information which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. To meet such situation, it is necessary that the customers are educated and apprised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company.

To educate the customers, the Company will arrange FAQs on KYC and AML measures. Such FAQs may be made available to the customers directly, on request, or through the Company's website.

---XXX---