Mitrata Inclusive Financial Services Ltd.

Know Your Customer & Anti-Money Laundering Policy

APPLICABILITY

This "Know Your Customer and Anti-Money Laundering Policy" (**the Policy**) will apply to **Mitrata Inclusive Financial Services 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 funding activities;
- 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 applicable laws.

VALIDITY

This Policy shall be effective from the date of approval of this policy. The Policy shall be reviewed as and when required by the applicable rules and regulations. 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;

DEFINITIONS

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

a) **Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (TargetedDelivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

b) "**Act" and "Rules**" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

c) "**Authentication**" in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

d) **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.

e) **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.

f) **Certified Copy** - Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act.

g) **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.

h) **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.

i) **"Digital KYC"** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act.

j) **Equivalent e-document"** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of thecustomer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

k) **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 of Address'.

l) **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 there under and includes:-

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".

m) 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.

n) **Non-face-to-face customers-** Customers who open accounts without visiting the branch/ offices of the Company or meeting its officials.

o) **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 of customers.

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 KYC verification.

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

q) **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 Rules thereunder.

r) **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 officials etc.

s) **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.

t) **'Senior Management'** for the purpose of KYC compliance shall include members of the Executive Committee, Designated Director, Principal Officer (PO) and his supervisor.

u) **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 to terrorism.

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.

v) **Transaction-** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a) opening of an account;

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-physical means;

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

d) entering into any fiduciary relationship;

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

f) establishing or creating a legal person or legal arrangement.

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

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 CDD procedure.

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 is opened.

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 and reported.

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 kept confidential.

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 be adopted.

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 a decision.

g) The Company may rely on third party verification subject to the conditions prescribed by Reserve Bank of India (RBI) in this regard.

h) The purpose of commencing the relationship/opening of accounts shall be established and the beneficiary of the relationship/account shall also be identified.

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 the following:

a) Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the RE;
b) Broad principles may be laid down by the Company for risk-categorisation of customers.
c) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
d) The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer

CUSTOMER IDENTIFICATION PROCESS

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/AQM/AM 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.

Customer Identification Procedures (CIP)

The Company shall undertake identification of customers in the following cases:

1. Commencement of an account-based relationship with the customer.
2. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
3. Selling their own products, selling third party products as agents and any other product for more than Rs.50,000/-.
4. Carrying out transactions for a non-account-based customer (walk-in customer).
5. The Company shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.
6. The Company shall obtain and verify Permanent account number (PAN) of customers as per the applicable provisions of Income Tax Rule 114B. Form 60 shall be obtained from persons who do not have PAN.
7. The documents to be accepted by the Company for customer identification shall be based on the regulatory prescriptions from time to time and shall be finalized after approval from Operations Head.
8. Decision-making functions of determining compliance with KYC norms shall not be outsourced.
9. The customers shall not be required to furnish an additional Officially valid document (OVD), if the Officially valid document (OVD) submitted for KYC contains proof of identity as well as proof of address.
10. The customers shall not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/ his local address on which all correspondence shall be made by the Company.
11. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as cheque books, ATM cards, telephonic conversation, positive address verification etc.
12. In case of change in the address mentioned on the 'proof of address', fresh proof of address should be obtained within a period of 6 months.

Detailed Procedure is enclosed as **Annexure A** to this Policy.

CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

The Company shall obtain the following documents from an individual while establishing an account based relationship:

i) one certified copy of an (OVD) as defined above containing details of identity and address.

ii) one recent photograph; and

iii) such other documents pertaining to the nature of business or financial status

specified by the Company.

Further, the Company shall carry out authentication of the Customer's Aadhar Number using e-KYC authentication facilities provided by the Unique Identification Authority of India. Moreover, where the customer has submitted an equivalent e document of any Officially valid document (OVD), the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and rules made thereunder and take a live photo as specified in Reserve Bank Of India (RBI) Circular.

2. The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

3. A copy of the marriage certificate issued by the State Government or Gazette notification indicating changein name together with a certified copy of the 'officially valid document' in the existing name of the personshall be obtained for proof of address and identity, while establishing an account-based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

4. If an existing KYC compliant customer of the Company desires to open another account with it, there shall be no need for a fresh CDD exercise provided there is no change in details last provided under the Company's KYC norms.

Where the Company is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR.

PROHIBITED LIST OF INDIVIDUAL/ENTITIES:

The Company shall ensure that in terms of Section 51A of Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, any of the existing or new customers are not in the prohibited list of individuals and entities which are periodically prescribed by local regulator from time to time. Compliance monitoring of such individuals / entities are done periodically be screening them against the below lists provided under RBI Directions, as amended from time to time:

(i) The "ISIL (Da'esh) & Al-Qaeda Sanctions List:

https://scsanctions.un.org/ohz5jen-al-qaida.html

(ii) The "Taliban Sanctions List":

https://scsanctions.un.org/3ppp1en-taliban.htm

Pursuant to the above screening, if any of the accounts of customers of individuals or entities are categorised as 'High-Risk', then the Company shall follow the enhanced due diligence procedures prescribed under RBI Directions

DIGITAL KYC PROCESS

A. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken onlythrough its authenticated application.

B. The access of the Application shall be controlled by the Company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice- versa. The original Officially valid document (OVD) shall be in possession of the customer.

C. The Company must ensure that the Live photograph of the customer is taken by the authorized officer andthe same photograph is embedded in the Customer Application Form (CAF). Further, the system Applicationof the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official'sname, unique employee Code (assigned by Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

D. The Application of the Company shall have the feature that only live photograph of the customer is capturedand no printed or video-graphed photograph of the customer is captured. The background behind the customerwhile capturing live photograph should be of white colour and no other person shall come into the frame whilecapturing the live photograph of the customer.

E. Similarly, the live photograph of the original Officially valid document (OVD) or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearlyreadable and identifiable.

F. Once the above mentioned process is completed, a One Time Password (OTP) message containing the textthat 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/knownpersons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer of the Company shall not be used for customer signature.

G. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with

the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

H. The authorized officer of the Company shall check and verify that:- (i) information available

in the pictureof document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.

I. On Successful verification, the CAF shall be digitally signed by authorized officer of the Company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

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.

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 EVALUATION

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 SENIOR MANAGEMENT

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.

RECORD MANAGEMENT

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---

Annexure A

Procedural Guideline

1. Branch staff must collect two Primary KYCs: **Voter ID and UID (Aadhaar)** qualify as Primary KYCs.

Primary KYC pool

S.No	Name of KYC
1	Voter's Identity Card
2	Aadhaar Card

2. Collection of **Voter ID is mandatory** for all the states.
3. FO will first enter Aadhar number in Finpage before uploading scan image of Aadhar.
4. 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.
5. If Aadhaar card number is uploaded with all numbers AMQ will immediately notify to FO/BM for necessary correction and get the correct image uploaded.
6. If after instruction from AMQ also, the correction is not done on Aadhar upload as stated in point no. four, HO credit will have the authority to hold the file and notify the BM on real time basis within maximum two hours.
7. In case Aadhaar ID is not available, branch staff can collect 2nd KYC from the secondary KYC pool.

Voter ID exception/deviation

8. In case if any client doesn't have Voter Id card but have Voter ID number in any documents like voter
   Slip etc. can be taken as a proof of primary KYC and cross checked at government electoral portal. If Voter ID number found correct on portal, then scan image of portal generated voter ID information can be uploaded in place of original Voter ID card. (This condition is non-negotiable. 20% cases for Voter Id as exception can be taken in a center. In terms of number of clients maximum two exceptions can be accepted in a center. (Exp- If there are five customers at the center, the voter slip of one customer can be taken. If there are more than five customers, two voter slips can be taken. Can't take more than that)
9. If above exception given to the clients (max. two in a center) it's mandatory to take third valid KYC from client in such cases. This KYC should have photo of client.

Secondary KYC pool

S.No	Name of KYC
1	Digital Ration Card
2	Driving License

3	Passport
4	Job Card by MNREGA

10. Photo ID proof of the **co-borrower** is required. Following documents can be collected for this

S.No.	Name of KYC	Issuing authority	Valid for		
			ID Proof	Age	Address
1	Aadhaar Card	UIDI	Yes	Yes	Yes
2	Voter ID	Election Commission of India	Yes	Yes	Yes
3	Digital Ration card	Government of India	No	Yes	Yes
4	MNREGA Job Card	State Govt.	Yes	No	Yes
5	PAN card	Income Tax Department	Yes	Yes	No
6	Driving License	Indian Union Driving License	Yes	Yes	Yes
7	Passport	Government of India	Yes	Yes	Yes

11. Residence Proof:

Incase current address of the customer is not captured in either of the two KYC documents submitted, then any of the following documents should be collected as Proof of Address in order of preference–

Any standard POI (Proof of ID) document which gives the address-

- Ration card, driving license, MGNREGA (Job) Card and passport
- Electricity Bill (less than 3 month sold)
- Digital Ration Card (without photo)
- House Tax Receipt (less than 2 years old)
- Bank Pass Book (printed only) which captures the customer's address

1. Acceptance level in case of Mismatch in Two KYCs

From two KYCs, submitted by the customers, we are to match the following parameters in both of them.

I. Customer's/ co-borrower's name

II. Customer's / co-borrower's Age or DOB

III. Address of Customer

IV. Name of Spouse

V. Photo of the customer

VI. Bank passbook account holder name

Please find the deviation score against such mismatch and the approval authority for such deviation cases

Name Mismatch:-

					Example	
Parameter	To be checked	Types of mismatch	Deviation score		KYC 1	KYC 2
		Mismatch in spelling but phonetics is same	0		Vinita Bharadwaj	Vinita Bharadwaj / VinithaBharadwaj
		Name is different, court affidavit and paper ad given	0		Vinita Bharadwaj	VibhaSen
		Sur name is different, because of change in surname after marriage, (Husbands KYC is to be taken and the surname of the husband is to match with that of wife's surname after marriage or marriage	0		Vinita Bharadwaj	Vinita Sharma

		certificate is taken)				
Name	VID against Adhaar	Difference in spelling in one instance and phonetics is different	1		Vinita Bharadwaj	VijitaBharadwaj
		Surname is missing	1		Vinita Bharadwaj	Vinita
		Only surname is different	2		Vinita Bharadwaj	Vinita Pal
		Name is different	3		Vinita Bharadwaj	Vibha Sen
Photo	KYCs against photo and person in physical	Photo is different	3			
		Age as per both KYC to be between 21 to 58	0			
Date of Birth	Age as on date	Age not within 21 to 58 in any one of the KYC	3			
					POA	**CurrentPhysical Address**

		Part address is mismatching but pincode is matching	1		228, AMBEDKAR WARD, KHARGAPUR, TIKAMGARH, MP 472115	220, GYAN WARD, KHARGAPUR, TIKAMGARH, MP 472115
		Address is same but Pincode is not matching	0		228, AMBEDKAR WARD, KHARGAPUR, TIKAMGARH, MP 472115	228, AMBEDKAR WARD, KHARGAPUR, TIKAMGARH, MP 472114
Address matching criteria	Declared POA against current physical address	Address is different but District and Pincode is matching	2		228, AMBEDKAR WARD, KHARGAPUR, TIKAMGARH, MP 472115	410, SULTANPUR WARD, JITAN NAGAR, TIKAMGARH, MP 472115
		Address and pincode mismatch	3		228, AMBEDKAR WARD, KHARGAPUR, TIKAMGARH, MP 472115	552, JODHBAI WARD, SIHORA, JABALPUR, MP 482004
					KYC 1 / KYC 2	**Father's / Husband;s KYC**
		Mismatch in spelling but phonetics is same	0		Jitram Patel	Jeetram Patel
		Name is different, court affidavit and paper ad given	0		Jitram Patel	Ganesh Chand
	Female: Any one POI against KYC of (Husband / Father),	Difference in spelling in one instance and phonetics is different	1		Jitram Patel	Jotram Patel

Father's/ Husband's name	Male: Any one POI against KYC of Father	Surname is missing	1		Jitram Patel	Jitram
		Only surname is different	2		Jitram Patel	Jitram Sharma
		Name is differe nt	3		Jitram Patel	Ganesh Chand
					KYC 1 / KYC 2	Bank Passbook
Bank Account Holder Name matching criteria	KYC1/KYC2 borrower's name against bank account holder's name should match	Name is differen t	3		Vinita Bharadwaj/Vinita	Sunita
		Borrower' s photo is not available in Bank passbook	1			
		Printed passbook without stamp and sign	1			
		Hand written Passbooks with bank stamp and signature	1			
		Hand written Passbooks without bank stamp and signature	3			

Parameter deviation score and Approving authority			
Highest of any parameter deviation score	**Status**	**Approving Person**	
1	Deviation	AMQ (Area Manager Quality)	Field Level
2	Deviation	Credit Manager	HO level
3	Reject	Reject	

Procedural Guidelines

1. Key demographic details of the Client (name, age/dob, father/spouse name, address) should be captured from Aadhar ID. The cases where Aadhar card is not available the same data should be captured from the Voter ID card.
2. All the above instructions are applicable for all branches.
3. BM and AMQ should check Original KYC and Bank passbook at the time of any Primary Loan sanction.
4. If there is any mismatch in the village in customer both kyc the center will hold and the AMQ will verify the same before approve/sanction the loan of customer.
5. Any VID/UID which is create/download on same day will be not acceptable. If the borrower and co- borrower have any old kyc which is matched with recent KYC can be considered for loan process.
6. If there is any mismatch in the polling booth in VID hard copy and online portal the AMQ will verify the same and reject/approve the client.
7. If there is any mismatch in the state in VID/UID hard copy and online portal that time client will be rejected.