SATYA MICROCAPITAL LIMITED

Know Your Customer (KYC) and Anti- Money Laundering (AML) Policy

Version 3.0

Document review and approval

Name of the document	Know Your Customer (KYC) and Anti- Money Laundering (AML) Policy
Approving Authority	Board of Directors
Date of Approval	May 29, 2026
Effective date of the Policy	Board approval date
Policy making body	Compliance department
Finalized/Reviewed by	Choudhary Runveer Krishanan, CS & CCO
Review Frequency	Annually and upon need basis
Version No.	3.0

Version Control

Sr. No.	Version No.	Revision remarks	Effective Date	Approved by
1.	1.1	First Approval	05-01-2018	Board of Directors
2.	2.0	Align as per the amended RBI master direction Know Your Customer	13-11-2021	Board of Directors
3.	2.1	Align as per the amended RBI master direction Know Your Customer	11-08-2023	Board of Directors
4.	2.2	Align as per the amended RBI master direction Know Your Customer	19-01-2024	Board of Directors
5.	2.3	Align as per the amended RBI master direction Know Your Customer	12-08-2025	Board of Directors
6.	2.4	Align as per the amended RBI master direction Know Your Customer	14-11-2025	Board of Directors
7.	3.0	Align as per the Revised master directions KYC, 2025	29-05-2026	Board of Directors

1. Introduction

SATYA MicroCapital Limited is a Public Limited Company incorporated under the provisions of the Companies Act, 1956 and validly existing under the provisions of the Companies Act, 2013, (hereinafter referred to as "SATYA" or the "Company"). SATYA is a Non-Deposit taking Non-Banking Financial Company ("NBFC"") registered and regulated by the Reserve Bank of India ("RBI") as a Non-Banking Financial Company – Micro Finance Institution ("NBFC - MFI") bearing Registration no. 14.01513.

The Company is engaged in the business of providing primarily Microfinance Loans and other loan products to borrowers from low-income households, primarily in rural and semi-urban areas, which include Water & Sanitation loans, Micro, Small and Medium Enterprises Business loans, Limited liability loans, etc. The Company focuses on empowering rural women both digitally and financially and facilitate financial inclusion.

2. Objective & Scope

The primary objective of this policy is to ensure strict compliance with the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 (hereinafter referred to as the 'KYC Directions'), as amended from time to time, along with the Prevention of Money-Laundering Act, 2002 (PML Act), and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules). This policy also ensures adherence to applicable sanctions regulations, thereby preventing the misuse of SATYA funds for any unlawful or prohibited activities. Furthermore, it seeks to protect the integrity and security of SATYA's financial systems by effectively combating money laundering, terrorist financing, and related threats. This Policy requires the Company and each employee to:

- Protect the Company from being used for money laundering or funding terrorist activities.
- Conduct themselves in accordance with the highest ethical standards.
- Comply with the letter and the spirit of applicable Anti-Money Laundering (AML) Laws, and the Company's KYC & AML procedures.
- Be alert to and escalate suspicious activity and not knowingly provide advice or other assistance to individuals who attempt to violate or avoid money-laundering laws, or this Policy; and
- Co-operate with the regulatory authorities and the Financial Intelligence Unit as per the applicable laws.

Scope:
This policy applies to all employees, customers, agents, and associates of SATYA engaged in financial transactions or associated processes. The scope of this policy covers:

- To lay down explicit criteria for acceptance of customers.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

To fulfil the scope, the following four key elements will be incorporated into our policy:

- Customer Acceptance Policy
- Risk Management
- Customer Identification Procedures
- Monitoring of Transactions

3. Validity of the Policy

The Board shall review, validate, update, and approve the Policy as applicable from time to time. Any

revisions in specific aspects of this Policy may be communicated through mandates issued by the relevant authority and shall become part of this Policy from the date they become effective.

4. Definitions

In this policy, unless the context otherwise requires, the terms herein shall bear the same meanings assigned to them under the Reserve Bank of India Act, 1935, KYC Directions, PML Act, PML Rules, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto. For the purpose of KYC Norms, definition of various terms used is as under:

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

1.2 "**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.

1.3 **"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.

1.4 **Beneficial Owner (BO)**

(a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

i) "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.

ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

(b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control (including right to control the management or policy decision) through other means.

(c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

1.6 **"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 documents produced by the customer with the original and recording the same on the copy by the authorized officer of the RE as per the provisions contained in the Act. In the case

of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), the Company may alternatively obtain the original certified copy of documents. Such certification can be provided by any one of the following authorities- Authorised officials of overseas branches of Scheduled Commercial Banks registered in India; branches of overseas banks that maintain relationships with Indian banks; a Notary Public abroad; a Court Magistrate; a Judge; or the Indian Embassy or Consulate General in the country where the non-resident customer resides.

1.7 **"Counterfeit Currency Transaction** means 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.

1.8 **Customer**" means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

1.8 **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'. The sources of identification should be reliable and independent. The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

(c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

1.9 **"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.

1.10 **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

1.11 Deemed OVD Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

The customer shall submit OVD with current address within a period of three months of submitting the deemed OVD.

Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address

1.11 **"Designated Director"-** means a person designated by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act (PMLA) and the Rules thereunder and includes:-

a) The Managing Director or a Whole-Time Director duly authorized by the Board of Directors,

b) The name, designation and address of the Designated Director shall be communicated to the Financial Intelligence Unit-India (FIU-IND).

c) The Principal Officer of the company should not be nominated as the "Designated Director".

1.12 **"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 the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

1.13 **e-KYC Authentication Facility** means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through an entity, is matched against the data available in the Central Identities Data Repository (CIDR), and the Unique Identification Authority of India returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction;

1.14 **Financial Intelligence Unit – India (FIU-IND)** It is the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. It is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. It is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the finance minister.

1.15 **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

1.16 **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the Central KYC Records Registry (CKYCR), for individuals and legal entities, as required by the relevant Rules.

1.17 **Non-face-to-face customers** means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of Company

1.18 **"Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

1.19 **"Officially Valid Document" (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address or any other document as notified by the Central Government in consultation with the Regulator.

1.20 **"On-going Due Diligence"** - Regular monitoring of transactions in accounts to ensure that they are consistent with the Company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

1.21 **"Politically Exposed Persons" (PEPs)** are individuals who are or have been entrusted

with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

1.22 **Principal Officer (PO)**

a) An official at the management level designated by the Board of Directors of the Company for overseeing and managing the KYC& AML policies and processes.
b) The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
c) The name, designation and address of the Principal Officer shall be communicated to the Financial Intelligence Unit-India FIU-IND.

1.23 **"Senior Management"** - for the purpose of KYC compliance shall include Management Committee which comprises of Head of Departments including Dy. Chief Executive Officer (if any) & Chief Financial Officer, Designated Director, Principal Officer (PO), etc.

1.24 **"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 proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

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

c. appears to not have 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.

1.25 **"Video based Customer Identification Process (V-CIP)"**: a method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio- visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

5. Money Laundering and Terrorist Financing Risk Assessment by the Company:

a) The Company shall carry 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. as applicable from time to time.

b) The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

c) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. The periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However risk assessment should be reviewed at least annually.

d) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

e) The Company shall ensure to undertake the ML/TF risk assessments prior to the launch / use of new products, new business practices, services, technologies; and adopt a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

6. The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. The Company shall implement Customer Due Diligence (CDD) programme pertaining to ML/TF risks identified and the size of the business. Further, the Company shall monitor the implementation of the controls and enhance them If necessary.

7. Customer Acceptance Criteria

In line with the KYC Directions, the Prevention of Money Laundering Act (PMLA) and the Rules thereunder, the Company has formulated Customer Acceptance Policy (CAP) which lays down the broad criteria for acceptance of customers:

The features of the Customer Acceptance Policy (CAP) are detailed below:

a) The Company shall not open any account(s) in anonymous, fictitious or 'benami' name(s).

b) No account will be opened where the Company is unable to apply appropriate due diligence measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR if necessary when it is unable to comply with the relevant CDD measures in relation to the customer.

c) No transaction or account-based relationship shall be undertaken without following the due diligence procedure.

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

e) 'Optional'/additional information, will be obtained with the explicit consent of the customer after the account is opened.

f) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

g) CDD Procedure will be followed for all the joint account holders, while opening a joint account.

h) The Company shall 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 Reserve Bank of India (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 to FIU.

i) Adequate due diligence is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company shall conduct appropriate due diligence.

j) The Company may rely on third party verification subject to the conditions prescribed in the

KYC Directions in this regard.

k) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority

l) For non-face-to-face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised for identification and verification of such customers.

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

n) The information collected from the customer shall be kept confidential.

o) Appropriate Enhanced Due Diligence (EDD) measures shall be adopted for high risk customers from AML perspective, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically Exposed Persons (PEPs) and their family members/close relatives.

p) 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/freezing 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.

q) Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

r) Where GST number is available, the same shall be verified through the search/verification facility provided by the issuing authority.

s) The Company shall not deny financial facilities to any members of the general public, especially to those who are financially or socially disadvantaged, including Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

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.

8. Video based Customer Identification Process (V-CIP):

The Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account-based relationship with an individual customer, for updation/ periodic updation of KYC for eligible customers and for conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication after obtaining his informed consent.

V-CIP Procedure:

i) The official shall carry out liveness check during the V-CIP process and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii) During V-CIP, disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop / disconnection, fresh session shall be initiated.

iii) Any prompting observed at end of customer shall lead to rejection of the account opening process.

iv) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at

appropriate stage of workflow of V-CIP process.

v) The authorized official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
- OTP based Aadhaar e-KYC authentication
- Offline Verification of Aadhaar for identification
- KYC records downloaded from CKYCR, using the KYC identifier provided by the customer
- Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.

vi) The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

vii) Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India.

viii) The official shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

ix) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement.

x) It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

xi) The official shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

xii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 working days from the date of carrying out V-CIP.

xiii) The Company shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document.

xiv) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

xv) The Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio- visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt.

xvi) The Company shall ensure to redact or blackout the Aadhar Number obtained from the client.

V-CIP Infrastructure:

The Company opting to undertake V-CIP, shall adhere to the following minimum standards:

- The technology infrastructure supporting V-CIP must be hosted within the Company's own premises, with all V-CIP connections and interactions originating exclusively from the Company's secured network domain.
- In cases where cloud deployment models are employed, ownership of all data including video recordings shall remain exclusively with the Company. Such data shall be immediately transferred to the Company's owned or leased servers (including cloud servers) upon completion of the V-CIP process, and must not be retained by any cloud service provider or third-party technology vendor.
- The Company shall ensure end-to-end encryption of data flowing between the customer's device and the V-CIP application hosting environment shall be ensured in accordance with accepted encryption standards.

- The Company shall document customer consent in a manner that is auditable and tamper-proof.
- The V-CIP infrastructure/application shall incorporate mechanisms to block connections originating from IP addresses outside India or from spoofed IP addresses, thereby strengthening security controls.
- The application shall integrate advanced capabilities such as facial liveness detection, spoof prevention, and high-accuracy facial matching technologies. While AI-driven tools may be leveraged to enhance robustness, the ultimate responsibility for accurate customer identification rests with the Company.
- The technology ecosystem supporting V-CIP including application software and operational workflows shall be subject to continuous improvement based on periodic assessments of detected, attempted, or near-miss cases of identity forgery. Any confirmed incidents of forged identities identified through V-CIP must be reported promptly as cybersecurity events.
- Prior to deployment, the V-CIP infrastructure shall undergo comprehensive security evaluations including Vulnerability Assessments, Penetration Testing, and Security Audits to validate robustness and encryption efficacy. Critical vulnerabilities identified during these assessments must be addressed before implementation. Such testing shall be conducted by auditors empanelled with the Indian Computer Emergency Response Team (CERT-In).
- To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

V-CIP Records and Data Management:

- The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search.
- The activity log along with the credentials of the official performing the V-CIP shall be preserved.

9. Risk Management Framework:

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

9.1 Risk Based Approach:

a) Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company.
b) Broad principles may be laid down by the Company for risk-categorization of customers.
c) Risk categorization 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 categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Indicative parameters to categorize each customer into different risk-category is presented below:

- **Low-Risk Customers:**

  Low risk customers are characterized by strong identity integrity and consistent KYC compliance, where all submitted documents such as Aadhaar and PAN fully match without discrepancies. These individuals typically maintain stable financial profiles, with little to no existing indebtedness, low monthly repayment obligations, and a clean credit history with no overdue records. From a behavioural perspective, they demonstrate disciplined borrowing patterns, with minimal loan applications, no prior rejections, and no indicators of fraud risk. Additionally, they are generally located in low risk geographies and derive income from stable and verifiable sources such as agriculture, livestock, or established retail activities. For such

customers, standard onboarding procedures and routine monitoring frameworks are considered adequate.

- **Medium-Risk Customers:**

  Medium risk customers exhibit moderate risk due to minor inconsistencies or emerging financial and behavioural indicators. These may include small discrepancies in identity documentation, reliance on alternate OVDs, or moderate levels of indebtedness and repayment obligations. Such customers may have one or more active loans, limited credit exposure, or minor overdue records within acceptable thresholds. Behavioural signals, including multiple recent loan applications or past rejection history (typically within the last 3–6 months), may indicate evolving credit stress. Additionally, customers with seasonal or irregular income streams fall under this category. These profiles necessitate enhanced due diligence, closer verification of financial capacity, and periodic monitoring to mitigate potential risks.

- **High-Risk Customers:**

  High risk customers present significant concerns across identity verification, financial exposure, and behavioural indicators. This category includes individuals with major KYC discrepancies, missing mandatory documents, or mismatches identified during field verification. Financially, such customers often carry high levels of indebtedness, multiple active loans, elevated monthly obligations, and adverse credit bureau records, including overdues. Behavioural and fraud related red flags—such as MNRL matches, frequent or excessive loan applications in a short period, recent loan rejections, or inconsistent field observations—further elevate the risk profile. Additionally, customers operating in high risk geographies or engaged in cash intensive and irregular income activities are classified within this group. These cases require stringent onboarding controls, comprehensive verification, and continuous monitoring to effectively manage credit and fraud risks.

9.2 Monitoring:

- The Company shall consistently conduct on-going 'Due Diligence' to regularly monitor the transactions in accounts to ensure that those are consistent with Company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth. In addition to on-going monitoring, the Company shall ensure that following types of transactions are necessarily monitored:
  - Complex transactions and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
  - Transactions which exceed the thresholds prescribed for specific categories of accounts.
  - High account turnover inconsistent with the size of the balance maintained.
  - Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

- The monitoring shall be aligned with the risk category of the customer and therefore the Company shall ensure that:
  - A system of periodic review of risk categorization of accounts, at least once in six months, and enhanced due diligence measures, wherever required are put in place.
  - High risk accounts are subjected to more intensified monitoring.

- Monitoring of Customer Repayments: Identify patterns of delayed or missed payments that may indicate financial distress or potential fraud and review customers who repay loans unusually early, as this could be linked to suspicious funding sources.
- Manual and Automated Checks: Monitor repayment patterns using internal systems to flag anomalies and conduct periodic reviews of flagged accounts based on repayment inconsistencies or unusual customer behaviour.

  - Use manual/system-based checks to ensure loan utilization aligns with declared business activities. Cross-reference customer details with sanctions lists to ensure compliance.

- Customer data will be periodically checked against domestic and international sanctions lists and the screening will be performed during onboarding and at predefined intervals thereafter.

➢ Risk Indicators for Monitoring: Customers with repeated delays in repayments without valid explanations and loan usage patterns inconsistent with declared income or occupation.

10. List of Customer Identification Documents

Following documents are collected for customer identification and address verification:

1. Filling of KYC form and First Primary KYC document: Aadhar ID should be necessary ID for all loan disbursed for both borrower and co-borrower.

2. Second (secondary) KYC document:

    - Voter ID issued by Election Commission
    - Driver License (Not expired)
    - PAN Card or Form 60
    - Passport
    - Job card issued to the borrower by NREGA and signed by the state government

When the customer furnishes an OVD that does not have an updated address, the Company shall accept deemed OVD as defined above or the equivalent e-documents thereof to be OVDs for the limited purpose of proof of address. However, the customer shall submit OVD with current address within a period of three months.

11. 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).where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected;
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.

13. When a Company has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

12. Customer Due Diligence (CDD) Procedure

i. The Company shall obtain the following documents from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity

a) one certified copy of an (OVD) as defined above containing details of identity and address; or

b) the KYC Identifier with an explicit consent to download records from CKYCR;
KYC documents downloaded from the CKYCR, but whose validity has lapsed, are not to be used for KYC purpose such other documents pertaining to the nature of business or financial status specified by the Company and

c) one recent photograph; and

d) PAN or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

e) Other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents

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 KYC Directions.

ii. Where customer has submitted an OVD or proof of possession of Aadhaar number, where offline verification cannot be carried out, the Company shall carry out verification through digital KYC procedure as defined in this policy.

iii. 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.

iv. A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall 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.

v. 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.

*Note: Where the customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number***.**

The Company may rely on customer due diligence (in line with Para 22 of KYC Directions) done by a

third party to verify the identity of customers at the time of commencement of an account-based relationship, subject to the following conditions:

- Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
- Adequate steps are taken by the Company to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
- The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- The third party shall not be based in a country or jurisdiction assessed as high risk.
- The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

13. <u>Aadhaar OTP based e-KYC in non-face-to-face mode:</u>

The Company shall ensure compliance with the following conditions for the accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode:

- There must be a specific consent from the customer for authentication through Aadhaar OTP based e-KYC.
- As a risk-mitigating measure for such accounts, the Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar in accordance with the board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- Using such authentication, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification CDD as defined in this policy is carried out.
- If the CDD procedure as defined in this policy is not completed within a year, no further debits shall be allowed.
- A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other the Company. Further, while uploading KYC information to CKYCR, the Company shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- The Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

14. <u>Simplified procedure for opening accounts:</u>

In case a person who desires to open an account is not able to produce documents, as specified in CDD, the Company may at its discretion open accounts subject to the following conditions:

- The Company shall obtain a self-attested photograph from the customer.
- The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
- The account shall remain operational initially for a period of twelve months, within which CDD/ V-CIP as specified in this policy shall be carried out.
- Balances in customer's all accounts taken together shall not exceed rupees fifty thousand at any point of time and the total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
- Where limit for balance in accounts or total credit limits as specified above are breached, the customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed.

- The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed.
- The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per CDD procedures/ V-CIP as defined in this policy.

KYC verification once done by one branch/office of the Company shall be valid for transfer of the account to any other branch/office of the same Company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

15. CDD Measures for Identification of Beneficial Owner (BO):

For opening an account of a Legal Person who is not a natural person, the Beneficial Owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the PMLA Rules to verify his/her identity shall be undertaken keeping in view the following:

(i) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) is a subsidiary of such listed entities , it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

(ii) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

16. Enhanced Due Diligence (EDD) Procedure for high-risk accounts:

- **Objective of EDD:**
  - To mitigate the elevated risks posed by high-risk accounts.
  - To prevent the Company from being exploited for illicit purposes while ensuring regulatory compliance.
  - To maintain institutional integrity by ensuring that all high-risk relationships are carefully monitored and managed.
- **Non-face-to-face customer:**

Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by Company for non-face-to-face customer onboarding (other than customer onboarding in terms Aadhaar OTP based e-KYC in non-face-to face mode):

- In case Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding.
- In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. The Company shall have a Board

approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

- Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

➢ **Politically Exposed Persons (PEPs):**

The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

- The Company have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP.
- Reasonable measures are taken by the Company for establishing the source of funds / wealth.
- The approval to open an account for a PEP shall be obtained from the senior management.
- All such accounts are subjected to enhanced monitoring on an on-going basis.
- In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship.

Note: These above instructions shall also be applicable to family members or close associates of PEPs.

17. <u>Central KYC Records Registry (CKYCR):</u>

CKYCR serves as a centralized repository for KYC records, enabling financial institutions to access verified customer information quickly and efficiently. The Company shall adhere to the following while using CKYCR:

- The Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the customer as the case may be.
- Whenever the Company obtains additional or updated information from any customer, the Company shall within seven days, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. Once CKYCR informs the Company regarding an update in the KYC record of an existing customer, the Company shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Company.
- The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

18. <u>Streamlined processes for KYC-compliant customers:</u>

➢ Customers who have already completed their KYC process with a regulated entity are no longer required to repeat the entire procedure for opening new accounts or availing of additional services with the Company. In such cases, for the purpose of establishing an account-based relationship, updation/ periodic updation or for obtaining KYC Records, the Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if

available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless:

- there is a change in the information of the customer as existing in the records of CKYCR; or
- the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
- the validity period of downloaded documents has lapsed; or
- the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

19. Combating Financial Terrorism

Screening Process: The Company shall do crossmatch analysis to verify customer details (e.g., name, date of birth, identification numbers, etc.) against the applicable sanction lists mentioned below to identify & eliminate the matched customers and take actions as prescribed under KYC Directions.

A. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

a. The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

i. The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at **www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list.**

ii. The **"Taliban Sanctions List"**, established and maintained pursuant to Security Council resolution 1988 (2011)**,** which includes names of individuals and entities associated with the Taliban is available at **https://www.un.org/securitycouncil/sanctions/1988/materials**.

b. The Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

c. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021.

d. **Freezing of Assets under section 51A of UAPA, 1967:** The procedure laid down in the UAPA Order dated February 2, 2021, shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

B. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

i. Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 01, 2023, by the Ministry of Finance,

Government of India (Annex III of the KYC Master Direction).

ii. Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

iii. Company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

iv. Company shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.

v. In case of match in the above cases, company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005.
A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI.

vi. In case of doubt, company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

vii. In case an order to freeze assets under Section 12A is received by the company from the CNO, Company shall, without delay, take necessary action to comply with the Order.

viii. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

C. Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-C. DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

D. In addition to the above, Company shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of section 51A of the UAPA and section 12A of the WMD Act.

E. Company shall undertake counter measures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

20. 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 only through 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.

D. The Company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, 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.

E. The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The

background behind the customer while capturing live photograph should be of white color and no other person shall come into the frame while capturing the live photograph of the customer.

F. 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 clearly readable and identifiable.

G. Once the abovementioned process is completed, a One Time Password (OTP) message containing the text that '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/known persons 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.

H. 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.

I. The Application shall give information about the completion of the process and also generate the transaction-id / reference-id number of the process. The authorised officer shall intimate the details regarding transaction-id / reference-id number to the customer for future reference.

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

21. 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.

Authentication of Aadhaar

In line with The Aadhaar (Authentication and Offline Verification) Regulations, 2021 the following guidelines shall be adhered to by the Company:

- Information to the Aadhaar number holder**:** At the time of authentication or Offline Verification using the Aadhaar Number, the Company shall inform the borrower, the following details and shall obtain the consent of the borrower in physical or electronic form and maintain logs or records of the consent:
  - the nature of information that Company will receive upon authentication from Aadhaar authority.
  - the uses to which the information received during authentication or offline verification may be put; and
  - alternate and viable means of submission of identification and that no service will be denied for refusing to, or being unable to, undergo authentication or offline verification provided that the customer is able to identify himself through a viable alternative means suggested by the requesting entity.
- The Company shall ensure that the information above is provided to the borrower in local language as well.

22. <u>Periodic KYC Updation</u>

The Company shall ensure that periodic updation of KYC is carried out for all customers as per risk categorization and the timelines prescribed under KYC Directions.

The Company may also update customer's KYC information/records based on the update notification received from CKYCR, provided requisite consent as prescribed is available with the Company.

KYC identifier as provided by CKYCR shall be the first reference point for the purpose of establishing an account-based relationship or verification of identity of Customers. Such option should be provided to the customers at the time of onboarding.

To ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. Periodic updation shall be carried out at least once in:

- every two years for high-risk customers
- every eight years for medium risk customers
- every ten years for low-risk customers

The timelines prescribed above shall apply from the date of opening of the account / last KYC updation. Further, the Company shall undertake updation /periodic updation of KYC as per the below guidelines:

- Individual Customers:
  - No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company's digital channels (such as mobile application of the Company), letter etc.
  - Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company's, digital channels (such as mobile application of the Company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. The Company may also obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer at the time of periodic updation.
  - Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

- Additional measures:
  - The KYC documents of the customer as per the current CDD standards shall be available with the Company. This shall be applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
  - Customer's PAN details, if available with the Company, shall be verified from the database of the issuing authority at the time of periodic updation of KYC.
  - Acknowledgment shall be provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
  - In order to ensure customer convenience, the Company may consider making available the facility of periodic updation of KYC at any branch.
  - Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment

of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents within 30 days therefrom.

- Notices for Periodic Updation of KYC:
  - The Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded in the Company's system against each customer for audit trail.
  - In case of existing customers, the Company shall obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, failing which the Company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer provided that:
    - Before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard.
    - Appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes subject to enhanced monitoring.

Customer may be onboarded in face to face mode through Aadhar biometrics-based e-KYC authentication and, in such cases, if the customer address, different from the address as per the identity information available in the UIDAI database (i.e. Central Identities Data Repository), the same shall be permitted post submission of self-declaration for such address by the Customer, if customers wants to. The Company shall perform all actions/activities who undertake periodic updation exercise as stipulated under the KYC Directions.

23. Reporting Obligations:

23.1 In accordance with the requirements under Rule 7 of PML (Maintenance of Records) Rules, 2005, , the Company shall furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU- IND):

a) **Cash transaction report (CTR)/Counterfeit Currency Report (CCR)** – All such cash transactions where forged or counterfeit Indian currency notes of bank notes have been used as genuine as Counterfeit Currency Report (CCR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.

b) **Suspicious Transactions Reporting (STR)-** The Company shall 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 Financial Intelligence Unit-India (FIU-IND).

c) The Company shall 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.

d) Where Company is carrying out V-CIP process, it shall ensure that any detected case of forged identity through V-CIP shall be reported as a cyber event.

e) As part of effective identification and reporting of suspicious transactions, robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use.

f) Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND in addition to advising the Ministry of Home Affairs (MHA)

23.2. Confidentiality and Prohibition against disclosing Suspicious Activity Investigations and Reports-

The Company shall maintain utmost confidentiality in investigating suspicious activities and while reporting Counterfeit Currency Report (CCR)/ Suspicious Transactions Report (STR) to the Financial Intelligence Unit-India (FIU-IND)/ higher authorities. However, the Company may share the information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local government authorities etc.

24. Sharing KYC information with Central KYC Records Registry

The Company shall capture the KYC information for sharing with the Central KYC Records Registry (C-KYCR) in the manner as prescribed in the Rules as per the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company shall upload the KYC data pertaining to all types of prescribed accounts with Central KYC Records Registry (CKYCR), Within 10 days of commencement of an account-based relationship with the customer. as per the Operational Guidelines for uploading the KYC data issued CERSAI.

25. Unique Customer Identification Code:

The Company shall allot an Unique Customer Identification Code (UCIC) while entering into new relationships with Individual customers as also the existing customers of the Company.

26. 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.

27. Responsibilities of Senior Management

27.1. Designated Director- The Company shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the Act 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".

27.2. 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 shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

28. Key Responsibilities of the Senior Management

a) Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under Act and Rules.

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

29. Record Management

29.1 The Company shall introduce a system of maintaining proper record of transactions required under PMLA and PML Rules as mentioned below:

a) 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.
b) All suspicious transactions whether or not made in cash.
c) Records pertaining to identification of the customer and his/her address; and
d) Should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

29.2 For maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. The Company shall,

a) maintain for at least 5 years from the date of transaction between the Company and the client, both domestic and international.

b) maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions so as to permit reconstruction of individual transactions, including the following:

(i) the nature of the transactions.
(ii) the amount of the transaction and the currency in which it was denominated.
(iii) the date on which the transaction was conducted, and
(iv) the parties to the transaction.

30. Hiring of Employees, their Training and Education of Customers

30.1 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 shall be put in place.

30.2 The Company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

30.3 On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.

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 a 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.

31. Secrecy Obligations and Sharing of Information:

(a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.

(b) 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.

(c) While considering the requests for data/information from Government and other agencies, the Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. the interest of the Company requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.