KYC & AML POLICY

VERSION CONTROL:

Version	Date of Adoption	Change Reference	Owner	Custodian	Approving Authority
1.0	16-Apr-2014	Know Your Customer (KYC) Policy and Anti-Money Laundering (AML) Measures drafted and approved by the Board	Compliance Team	Compliance Team	Board of Directors
1.1	08-May-2019	KYC Policy and AML Measures reviewed and updated as per Master Directions of RBI	Compliance Team	Compliance Team	Board of Directors
1.2	22-Jun-2021	KYC Policy and AML Measures reviewed and updated as per Master Directions of RBI	Compliance Team	Compliance Team	Board of Directors
1.3	03-Aug-2022	KYC Policy and AML Measures reviewed and updated w.r.t. AML screening mechanism	Compliance Team	Compliance Team	Board of Directors
1.4	29-May-2023	KYC and AML policy reviewed and updated as per Master Directions of RBI	Compliance Team	Compliance Team	Board of Directors

Important Note:

If at any time a conflict of interpretation / information between this Policy and any Regulations, Rules, Guidelines, Notifications, Clarifications, Circulars, Master Circulars/ Directions issued by Reserve Bank of India, from time to time, arise then interpretation of such Regulations, Rules, Guidelines, Notifications, Clarifications, Circulars, Master Circulars/ Directions issued by Reserve Bank of India, from time to time, shall prevail.

INDEX

1. PREAMBLE:

The Reserve Bank of India (RBI) has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML)/Combating Financing of Terrorism (CFT) measures and has advised all NBFCs to ensure that a proper policy framework on KYC and AML/CFT measures be formulated and out in place with the approval of the Board.

The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risk prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

The Company policy framework shall seek to ensure compliance with PML/AML Rules, including regulatory instructions in this regard and shall provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, the Company may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

This policy is applicable to all categories of products and services offered by the Company.

2. DEFINITION:

a. Beneficial Owner (BO) means BO as per table below**:**

Sr. No	Type of Customer	Persons to be considered Beneficial Owners (BO)
a	**Company**	Natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means. Explanation- For the purpose of this sub-clause- 1. "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company. **2.** "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	**Partnership Firm**	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 capital or profits of the partnership.

c	**Unincorporated association or body of individuals**	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	**Trust**	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.

b. **Certified Copy:** 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 Company. In the case of Non-Resident Indian (NRI)/Person of Indian Origin (PIO) customers, the following officials also could certify the copy of the OVD:

a. Authorized officials of overseas branches of Scheduled Commercial Banks registered in India;
b. Branches of overseas banks with whom Indian banks have relationships;
c. Notary Public abroad;
d. Court Magistrate;
e. Judge;
f. Indian Embassy/Consulate General in the country where the non-resident customer resides.

c. **Central KYC Records Registry (CKYCR):** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

d. **Customer:** A 'Customer' is defined as hereunder:

- A person or entity that maintains an account and/or has a business relationship with the Company;
- One on whose behalf such relationship is maintained (i.e., beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law; and
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company, say a wire transfer or issue of a high value demand draft as a single transaction.

e. **Customer Due Diligence (CDD):** means identifying and verifying the customer and the beneficial owner.

f. **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.

g. **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.

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

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

j. Non-profit organisations (NPO): means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961, that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

k. **Officially valid document (OVD)**: means the i) passport, 2) the driving licence, 3) proof of possession of Aadhaar number, 4) the Voter's Identity Card issued by the Election Commission of India, 5) job card issued by NREGA duly signed by an officer of the State Government and 6) letter issued by the National Population Register containing details of name and address. Provided that,

a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. However, the Company needs to ensure that the customers while submitting Aadhaar for Customer Due Diligence, redact or blackout their Aadhaar number in terms of sub-rule 16 of rule 9 of the amended PML Rules.

b) 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 license agreements with such employers allotting official accommodation;

c) The customer shall submit OVD updated with current address within a period of three months of submitting the documents specified in sub clause 'b' above.

d) 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.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

l. **Offline verification:** means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations as mentioned in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and

Services) Act, 2016 (18 of 2016).

m. Person: A 'Person' shall have the meaning as defined under KYC policy of RBI (and any amendment from time to time by RBI) which at present is as follows:
'Person' shall include:
a. an Individual;
b. a Hindu Undivided Family;
c. a Company;
d. a Trust
e. a Firm;
f. an association of persons or a body of individuals, whether incorporated or not;
g. every artificial juridical person, not falling within any one of the above person (a to e);
h. any agency, office or branch owned or controlled by any one of the above persons (a to f).

n. Politically Exposed Persons (PEPs): Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions by a foreign country, including theHeads of States/ Governments, Senior Politicians, Senior Government or judicial or military officers, Senior executives of State-Owned Corporations and Important political party officials. Company should gather sufficient information on any person / customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Company should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer.

o. 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.
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.

p. Video based Customer Identification Process (V-CIP): an alternate method of customer identification with facial recognition and Customer Due Diligence (CDD) by an authorised official of the Company by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face customer identification process for the purpose of this Policy. The scope, infrastructure and procedure for conducting the V-CIP is mentioned more particularly in **Annexure – 3**.

3. OBJECTIVES, SCOPE AND APPLICATION OF THE POLICY:

The primary objective is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities.

- To lay down explicit criteria for acceptance of customers.
- To establish procedures to verify the bona-fide identification of individuals/non- individuals for opening of account.
- 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.

4. KNOW YOUR CUSTOMER (KYC) STANDARDS:

To fulfil the scope, the Company hereunder framing KYC Policy incorporating the following four key elements:

4.1. Customer Acceptance Policy;
4.2. Customer Identification Procedures;
4.3. Monitoring of Transactions;
4.4. Risk Management.

4.1. CUSTOMER ACCEPTANCE POLICY ("CAP"):

The Customer Acceptance Policy (CAP) is developed laying down explicit criteria for acceptance of customers. The CAP shall ensure that explicit guidelines are in place on the following aspects of customer relationship in the Company:

a. Company shall not open any account in anonymous or fictitious / benami name(s) and where proper due diligence cannot be applied.
b. No transaction or account-based relationship is undertaken without following the due diligence procedure.
c. Parameters of risk perception shall be clearly defined in terms of the location of customer and his clients and mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into low, medium and high risk; customers requiring very high level of monitoring, e.g., Politically Exposed Persons shall be, categorized unfailingly in the high risk category. The Company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category - customer background, country of origin, sources of fund, banking experience and conduct, repayment track record of other lending, CIBIL check, availability of satisfactory financial records. The Company shall accept customers after verifying their identity as laid down in customer identification procedures. While carrying out due diligence the Company will ensure that the procedure adopted will not result in denial of services to the genuine customers;
d. The Company should ensure that documents and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002 (Central Act No. 15 of 2003) (hereinafter referred to as PMLA), rules framed there under and guidelines issued from time to time;
e. Not to open an account where the Company is unable to apply appropriate customer due diligence measures, i.e., the Company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It shall, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to close an account shall be

taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

f. Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practices, as there could be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in a fiduciary capacity;
g. Necessary checks before opening a new account so as to 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, caution list circulated by Reserve Bank of India, from time to time, etc.;
h. CDD procedure is to be followed for all the joint account holders, while opening a joint account.
i. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists as indicated in RBI KYC Master Directions.
j. The Company may leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements if an existing KYC compliant customer desires to open another account, there shall be no need for a fresh CDD exercise.
k. Additional Information, where such information requirement has not been specified in this policy, will be obtained with the explicit consent of the customer.
l. The Company shall apply CDD procedure at the Unique Customer Identification Code (UCIC) generation level while entering into new relationships with individual customers as also the existing individual customer. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, then there shall be no need for a fresh CDD exercise.
m. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
n. 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).
o. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

Risk Categorization:

The Company shall prepare a profile for each new customer based on risk categorization. The customer profile shall contain information relating to the customer's identity, social / financial status, nature of business activity, information about his clients' business and their location, geographical risk covering customers as well as transactions, type of products/ services offered, delivery channel used for delivery of product/ services, types of transaction undertaken- cash, cheque/monetary instruments, wire transfers, forex transactions, etc.. The nature and extent of due diligence will depend on the risk perceived by the Company. For the purpose of risk categorization of customer, the Company shall obtain the relevant/mandatory information from the customer at the time of account opening and during the periodic updation, for KYC purpose. However, while preparing customer profile, the Company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive and is in conformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with her/his/their consent and after opening the account.

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.

For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. Illustrative examples of low-risk customers would be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies, etc. In such cases, the policy shall require that only the basic requirements of verifying the identity and location of the customer are to be met.

Customers that are likely to pose a higher than average risk to the Company shall be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. The Company shall apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence shall include:

- non-resident customers;
- high net worth individuals;
- trusts, charities, NGOs and organizations receiving donations;
- companies having close family shareholding or beneficial ownership;
- firms with 'sleeping partners';
- politically exposed persons (PEPs) of foreign origin;
- non-face to face customers; and
- those with dubious reputation as per public information available, etc.

As regards the accounts of PEPs, in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company shall obtain senior management approval in such cases to continue the business relationship with such person, and also undertake enhanced monitoring.

The adoption of Customer Acceptance Policy and its implementation shall not become too restrictive and shall not result in denial of the Company's services to general public, especially to those, who are financially or socially disadvantaged.

Where the Company forms a suspicion 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 and STR with FIU-IND.

4.2. CUSTOMER IDENTIFICATION PROCEDURE ("CIP"):

Customer identification means identifying the customer and verifying her / his / its identity by using reliable, independent source documents, data or information while establishing a relationship. As per Rule 9 of the Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

a. at the time of commencement of an account–based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship; and
b. in all other cases, verify identity while carrying out:
    i. 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

ii. any international money transfer operations.

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The Company shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

The Company gets sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Rule 9 of the PML Rules provides for the documents/information to be obtained for identifying various types of customers i.e., individuals, companies, partnership firms, trusts, unincorporated association or a body of individuals and juridical persons. The Company taking note of the provisions of the above rule and shall ensure compliance. An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the **Annexure-1**. The internal guidelines based on the experience of dealing with such persons/entities, normal prudence and the legal requirements will also be considered.

Original Seen and Verified (OSV) Norms:

KYC documents provided by the customer (for applicant/co-applicant /guarantor and other related parties) will be sighted in original and verified by the Company's Employee/Sourcing Channel Partner, Fintech Partners and their employees who are authorized to do OSV and signed with "Original Seen and Verified" stamp.

Risk based approach is considered necessary to avoid disproportionate cost to the Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For customers that are natural persons, the Company will obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall:

a. verify the legal status of the legal person / entity through proper and relevant documents
b. verify that any person purporting to act on behalf of the legal person / entity is so authorized and identify and verify the identity of that person; and
c. understands the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

The Company has framed its own internal guidelines based on their experience of dealing with such persons/entities, normal lenders prudence and the legal requirements as per established practices. In case, customer is permitted to act on behalf of another person/entity, the same would be allowed only in conformity with established law and practices and after taking necessary safeguards such as notarizing the Power of Attorney or the mandate, KYC of both the customers and the authority operating the account including the intermediary acting in fiduciary capacity. The Company will take reasonable measures to identify the beneficial owner(s) and verify her/his/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

The document requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Official(s) in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales

and distribution channels and compliance.

Customer Identification Procedure shall be carried out at different stages i.e.:

- While establishing a business relationship (or)
- Carrying out any international money transfer operations for a person who is not an account holder of the Company (or)
- Carrying out a financial transaction (or)
- Where the Company has a doubt about the authenticity/veracity (or)
- Inadequacy of the previously obtained customer identification data if any (or)
- When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

No deviations or exemptions shall normally be permitted in the documents specified for account opening. In case of any extreme cases of exceptions, concurrence of Policy section shall be obtained duly recording the reasons for the same. Suitable operating guidelines for implementation of the KYC/AML guidelines shall be issued by the Company for its different business segments.

The Client Identification Programme is formulated and implemented to determine the true identity of its client keeping the above in view.

Important: The Company shall periodically review the risk categorization of loan assets, which shall not be less than once every 6 months. Company will also periodically update the customer identification data (including photograph/s) after the loan account is opened. The periodicity of such updation shall not be less than once in ten years in case of low-risk category customers; not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high-risk category customers.

Customer Due Diligence (CDD):

For undertaking CDD, the following documents should be obtained from the customer:

Sl. No.	Nature of the Document	Type of Verification
1	the Aadhaar number where he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the PML Act;	e-KYC authentication facility provided by the Unique Identification Authority of India
2	Proof of possession of Aadhaar number where offline verification can be carried out	Offline verification
3	Proof of possession of Aadhaar number where offline verification cannot be carried out	Digital KYC as specified under **Annexure-2**
4	Any OVD containing the details of identity and address	Offline verification through OSV or Digital KYC as specified under **Annexure–2**

5	Any equivalent e-document of any OVD containing the details of identity and address	Offline verification through OSV or through website of regulatory issuing authority or Verification of Digital signature and Live photo as specified under **Annexure-2**

Note: For a period not beyond such date as may be notified by the Government for the NBFCs, instead of carrying out Digital KYC, certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph (where an equivalent e-document is not submitted) may be obtained.

a. The KYC Identifier with an explicit consent to download records from CKYCR. Further, the Company can retrieve the KYC records online from CKYCR;
b. Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962;
c. The live V-CIP may be carried out by an official of the Company, for establishment of an account-based relationship with an individual customer, after obtaining informed consent with adherence to stipulations as per **Annexure-3**;
d. Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. Offline Verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

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

a. obtain a self-attested photograph from the customer;
b. 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.
c. The account shall remain operational initially for a period of twelve months, within which CDD shall be carried out.
d. Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.
e. The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
f. The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.
g. 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 in direction (d) and (e) above.

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 Company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

In case Accounts opened using Aadhaar OTP based e-KYC, in non-face to face mode, are subject to the following

conditions:

a. Specific consent from the customer for authentication through OTP to be obtained;
b. 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. The Company shall have board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts;
c. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
d. Accounts opened using OTP based e-KYC shall not be allowed for more than 1 year unless identification as mentioned above in table or through V-CIP is carried out. If Aadhaar details are used under V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
e. In case of opting this option, 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 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 companies shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
f. 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.

Enhanced Due Diligence Measures for non-face-to-face customer onboarding (other than customer onboarding as mentioned above):

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 for the purpose of this Section 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 the Company for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17 of Master Circular):

a. V-CIP shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP.

b. 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.

c. 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.

d. The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e. First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f. 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.

Customer Due Diligence (CDD) done by third party:

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:

a. Records or information of the customer due diligence carried out by the third party is obtained within 2 days from the third party or from the Central KYC Records Registry.
b. 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.
c. 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.
d. The third party shall not be based in a country or jurisdiction assessed as high risk.
e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

Updation/ Periodic Updation of KYC:

The Company shall adopt a risk-based approach for periodic updation of KYC.

Sr. No.	Type of Customer	Remarks
1.	**Individuals:**	
a.	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 or through letter.
b.	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 or through letter 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. Note: The Company may 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.

Sr. No.	Type of Customer	Remarks
c.	Aadhar OTP based e-KYC in non-face to face mode:	Aadhar OTP based e-KYC in non-face to face mode be used for periodic updation. The conditions stipulated in this policy w.r.t. accounts opened using Aadhar OTP based e-KYC in non-face to face mode are not applicable in case of updation / 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. The 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
2.	**Customers other than individuals:**	
a.	No change in KYC information:	In case of no change in the KYC information of the Legal Entity customer, a self-declaration in this regard shall be obtained from the Legal Entity customer through its email id registered with the Company or through letter from an official authorized by the Legal Entity customer in this regard or through board resolution etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.
b.	Change in KYC information:	In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

Additional Measures:

The Company shall undertake the following additional measures:

a. In case the KYC documents available with the company are not as per the current KYC standards and the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, then the Company undertake the KYC process equivalent to that applicable for on-boarding a new customer;
b. Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC;
c. An acknowledgment is 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;
d. In order to ensure customer convenience, the Company may consider making available the facility of periodic updation of KYC at any branch.
e. The 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 REs the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Company's' end.

4.3. MONITORING OF TRANSACTIONS:

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity attached with the client. The Company pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

For ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Company shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

Background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors shall determine the extent of monitoring. Higher risk accounts shall be subjected to intensify monitoring. Company shall carry out the periodic review of risk categorization of transactions/customers and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months.

The Company shall explore the possibility of validating the new accounts opening application with various watch lists available in public domain, including RBI watch list. After due diligence, any transactions of suspicious nature will be duly reported by Principal Officer to Director, Financial Intelligence Unit- India (FIU_IND).

Illustrative list of activities which would be construed as suspicious transactions:

- Activities not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
  - A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
  - Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
  - An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
- Some examples of suspicious activities/transactions to be monitored by the operating staff:
  i. Multiple accounts under the same name;
  ii. Refuses to furnish details of source of funds by which initial contribution is made, sources of fund are doubtful etc.;
  iii. There are reasonable doubts over the real beneficiary of the loan; and
  iv. Frequent requests for change of address.

To ensure monitoring and reporting of all transactions and sharing of information as required under the law for KYC, the Board may nominate any Director or authorized CMD or any other officer(s) duly authorized by CMD

to be designated as Company's Principal Officer with respect to KYC/ AML/ CFT.

The Company should adhere to the provisions of Income Tax Rules 114F, 114G and 114H and submit reports as per the process laid down under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Principal Officers for KYC/ AML/ CFT:

A Senior management officer would be designated as the Principal Officer(s) for KYC and will act independently and report directly to the concerned Director/MD or to the Board of Directors. The role and responsibilities of the Principal Officer(s) should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.

The collection of data on the borrower side would be the primary responsibility of Relationship and Operations team and the required data as per formats (Company Application Form) prescribed in this policy shall be collected, irrespective whether the Company is the lead institution or there are other co- financing institutions. To ensure monitoring of the KYC Guidelines laid down by the Company, the borrowers may be requested to resubmit their forms annually or in case there is any change in the structure of entity within 15 days of information of such change.

Details of the Principal Officer is mentioned in **Annexure-4**.

Designated Director:

The Managing Director of the Company is "Designated Director" who is responsible for ensuring compliance with the obligations under the PMLA, 2002 and rules.

Details of the Designated Director is mentioned in **Annexure-4**.

4.4. RISK MANAGEMENT:

The Board of Directors of the Company will ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with the Board, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti - Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

The adequate AML screening mechanism for mitigating risk for onboarding new customers and thereafter on annual basis is more particularly provided in **Annexure-5.**

The Company's internal audit and compliance functions shall have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function shall provide an independent evaluation of the Companies own policies and procedures including legal and regulatory requirements. The Company ensures that its audit machinery is staffed adequately with individuals who are

well-versed in such policies and procedures.

Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard will be put up before the Audit Committee of the Board at quarterly intervals. The Company shall ensure that there is proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines.

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.

The Company will have an ongoing employee training programme so that the members of the staff are adequately trained in KYC/AML/CFT procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

Risk Management Committee ("RMC"):

The Principal officer may submit the periodic report to RMC if a need arises in case of high-risk cases and which may require further guidance from Committee so they can assess the risk involved in the case of different customers on the basis of data collected by the business team. Depending on the requirement, services of an independent consultant having knowledge and background on the subject may be taken. Such issues of categorization shall be kept confidential and shall not be divulged to any third party irrespective of their relationship with Company at any level of organization.

5. MONEY LAUNDERING (ML) AND TERRORIST FINANCING (TF) RISK ASSESSMENT:

'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise should be carried out 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 shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time. Further, the internal risk assessment shall be carried in commensurate to its size, geographical presence, complexity of activities/structure, etc. Also, the Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and Board approved policies, controls and procedures should accordingly aligned. The Risk Assessment by the Company shall be properly documented and to be proportionate to the nature, size, geographical presence, complexity of activities/structure etc. of the Company. 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.

The Company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Further, the Company shall ensure: (a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and (b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and

transaction monitoring, etc.

6. CLOSURE OF ACCOUNTS/TERMINATION OF FINANCING/BUSINESS RELATIONSHIP:

Where Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-operation by the customer, the Company shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Managing Director or Principal Officer.

7. MAINTENANCE OF RECORDS OF TRANSACTIONS:

The Company will maintain proper record of transactions as required under section 12 of the PMLA read with Rule 3 of the PML Rules, as mentioned below:

7.1. all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

7.2. all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate value of such transactions exceeds rupees ten lakh or its equivalent in foreign currency;

7.3. all transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;

7.4. 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; and

7.5. all suspicious transactions whether or not made in cash and as mentioned in RBI guidelines / circulars / PMLA rules.

7.6. all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;

7.7. all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

7.8. V-CIP Records and Data Management:

7.8.1. The entire data and recordings of V-CIP shall be stored in a system(s) 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.

7.8.2. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

The Company will ensure that its branches continue to maintain proper record of all cash transactions of Rs.10 lakh and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling / head office on a fortnightly basis.

Information to be preserved:

The Company will maintain the following information in respect of transactions as referred to in the preceding point on "Maintenance of Records of Transactions:

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.

As per Section 12 of PMLA, the Company will maintain records as under:

a. records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules shall be maintained for a period of five years from the date of transactions between the customers and the Company.
b. records of the identity of all customers of the Company shall be maintained for a period of five years from the date of cessation of transactions between the customers and Company.

The Company will take steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows data to be retrieved easily and make available swiftly the identification records and transaction data whenever required or when requested by the competent authorities.

For the purpose of above, the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

8. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA:

The Company will report information of transaction referred to in clause (a) of sub-section (1) of section 12 of PMLA read with Rule 3 of the PML Rules relating to cash and suspicious transactions, etc., to the Director, Financial Intelligence Unit-India (FIU-IND). The Principal officer shall furnish information, where the principal officer of the Company has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of this section, in respect of such transactions to the Director within the prescribed time.

The formats for reporting the requisite information in respect of cash transactions and suspicious transactions as provided by FIU shall be followed as prescribed from time to time.

For determining integrally connected cash transactions, the Company shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds rupees ten lakh during the month.

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND immediately. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

The Company will pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose

thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. These records are required to be preserved for five years as is required under PMLA, 2002. Such records and related documents shall be made available to help auditors in their work relating to scrutiny of transactions and also to NHB/other relevant authorities.

It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. The Company shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

The Company shall make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall ensure that there is no tipping off to the customer at any level.

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967:

The procedure laid down in the UAPA Order dated 02-Feb-2021 (Annex II of KYC Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

9. COMBATING FINANCING OF TERRORISM:

a. In terms of PMLA Rules, suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The Company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

b. As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the Company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities shall be accessed from the United Nations website at: http://www.un.org/sc/committees/1267/consolist.shtml.

The Company shall before opening any new account, ensure that the name/s of the proposed customer does not appear in the list. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism including Know Your Employee/Staff Policy shall be put in place by the Company as an integral part of recruitment/hiring process of personnel.

The required information shall be furnished by the Company directly to the FIU-IND, through the Principal Officer designated by Company under the Prevention of Money Laundering Act, 2002.

10. OBLIGATIONS UNDER WEAPONS OF MASS DESTRUCTION (WMD) AND THEIR DELIVERY SYSTEMS

(PROHIBITION OF UNLAWFUL ACTIVITIES) ACT, 2005 (WMD ACT, 2005):

a. The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) 43 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 January 30, 2023, by the Ministry of Finance, Government of India.
b. The Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
c. The 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.
d. In case of match in the above cases, The 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. REs shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

In addition to the above, the 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

11. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR):

a. In terms of provision of Rule 9(1A) of PML Rules, 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.
b. The Company need to adhere operational guidelines released by CERSAI for uploading the KYC data.
c. Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
d. Once KYC Identifier is generated by CKYCR, Company shall ensure that the same is communicated to the individual or Legal Entities.
e. Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –
   i. There is a change in the information of the customer as existing in the records of CKYCR;
   ii. The current address of the customer is required to be verified;
   iii. The Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
   iv. The validity period of documents downloaded from CKYCR has lapsed.

12. SECRECY OBLIGATIONS:

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

Information collected from the Customer shall be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. The Company shall therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive and is inconformity with the guidelines issued by RBI in this regard. The Company shall ensure that account payee cheques for any person other than the payee constituent shall not be collected. The Company shall ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode for any amount is affected by cheques and not against cash payment. 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 nature as will violate the provisions of laws relating to secrecy in transactions.

13.REVIEW OF THE POLICY:

This policy shall be reviewedannually by the Management. If there is any change to the policy, then the Management will seek Board approval.

Annexure -1 - Customer Identification Procedure

Features to be verified and documents that will be obtained from customers

Customers/Clients	Documents (Certified Copy)
Individuals: Legal Name and any other names used Correct permanent address for proof of residence of individuals	a. Pan Card or form No.60 as defined in Income-Tax Rules, 1962; b. Passport; c. Voter's Identity Card; d. Driving License; e. Letter issued by Gazetted Officer with duly attested photograph of the individual; f. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company; g. Aadhaar card issued by Unique Identification Authority of India containing details of name, address and Aadhaar number; h. Utility bill, Telephone bill, Post paid broadband bill (not more than 2 months old); i. Account Statement latest 3 months; j. Letter from any recognized public authority; k. Electricity bill; l. Property/Municipal Tax Receipt; m. Piped Gas Connection Bill/Post Paid Mobile Bill (carrying the present address of the customer, provided that the said bills are not older than 2 months). n. Notarised/Registered rent agreement alongwith E-bill
Companies: -Name of the Company -Principal place of business -Mailing address of the Company -Telephone / Fax Number	Certified copies of the following documents: - a. Certificate of Incorporation (Mandatory); b. Memorandum of Association and Articles of Association (Mandatory); c. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf (Mandatory); d. The names of the relevant persons holding senior management position; e. The registered office and the principal place of business, if it is different; f. An officially valid document in respect of Mangers, Officers or Employee holding an attorney to transact on its behalf; g. Copy of PAN card (Mandatory); and h. Management/CA certified list of Directors and Shareholders (Mandatory) i. Copy of the Utility Bill/Postpaid Wifi bill (not older than 2 months). j. Letter/Certificate from any recognized public authority. k. GST/Govt Licenses and Establishment Certificates
Partnership Firm:	Certified copies of the following documents: - a. Registration certificate, if registered;

- Legal Name - Address - Names of all partners - And their address - Telephone numbers of the firm and partners	b. Copy of PAN Card; (Mandatory); c. Partnership deed (Mandatory); d. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf; e. The name of all the partners; f. Address of the registered, and the principal place of its business, if it is different; g. Any officially valid document identifying the partners and the persons holding the power of Attorney and their address; and f. Utility Bill (not older than 2 months) in the name of firms / partners g. Notarised/Registered rent agreement (proof of address) h. GST/Government approved Licences
Trusts & Foundation: - Name of trustees, settlers, beneficiaries and signatories - Name and address of the founder, the managers / directors and the beneficiaries - Telephone / fax numbers	Certified copies of the following documents:- a. Registration certificate, if registered; b. PAN Card or form No.60 as defined in Income-Tax Rules, 1962; (Mandatory); c. Trust deed (Mandatory); d. Power of Attorney granted to transact business on its behalf; e. The names of the beneficiaries, trustees, settlor and authors of the trust; f. The address of the registered office of the trust; g. List of trustees and documents, as specified in CDD procedure, for those discharging the role as trustee and authorised to transact on behalf of the trust. h. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders / managers / directors and their address; i. Resolution of the managing body of the foundation / association; and j. Utility Bill (not older than 2 months) in the name of trust / trustees.
Unincorporated Association or a Body of Individuals	Certified copies of the following documents: - a. Resolution of the managing body of such association or body of individuals; b. Power of attorney granted to him to transact on its behalf; c. Such information as may be required by the reporting entity to collectively establish the legal existence of such an association or body of individuals; d. An officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Sole Proprietary Firms/concerns Proof of the name, address and activity of the concern	Certified copy of OVD as applicable to the Individuals (i.e. of proprietor) shall be obtained. In addition to the above, any two of the following documents as a proof of business/activity in the name of the proprietary firm shall also be obtained: a. Registration certificate (in the case of a registered concern) including Udyam Registration Certificate (URC) issued by the Government. b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

	c. GST and Income tax returns. d. CST/VAT/GST certificate, whenever applicable Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities / GST authorities. e. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. f. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. g. Utility bills such as electricity, water, and landline telephone bills, post-paid wifi bills (not older than 2 months). h. Notarised/registered rent agreement alongwith E-bill. In cases where the Company is satisfied that it is not possible to furnish two such documents, it would have the discretion to accept only one of those documents as proof of business/activity. In such cases the Company, however would have to undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

In such cases the Company, however would have to undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

***Note**: Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.*

Annexure - 2 - Digital KYC Process

A. A Digital KYC Application for digital KYC process is to be made available at customer touch points and is to be undertaken only through this authenticated application of the Company

B. Access of the KYC Application to be controlled and be ensured that it is not used by any unauthorized person.

C. KYC App to be accessed only through Login-ID and Password, Live OTP or Time OTP controlled mechanism given to the authorized officials of the Company

D. Customer, for KYC, should visit the location of the authorized official of the Company or vice versa. The original OVD should be in possession of the customer

E. Live photograph of the customer should be taken by the authorized officer and the same photograph should be embedded in Customer Application Form (CAF).

F. KYC Application should add a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

G. KYC Application should have a feature such that only live photograph of the customer is captured and not printed or video-graphed photograph.

H. Background behind the customer should be white and no other person should come into frame.

I. Live photograph of original OVD or proof of possession of Aadhaar (if offline verification is not being done) placed horizontally, should be captured vertically from above and water-marking as stated above should be done. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.

J. Live photograph of customer and original documents should be captured in proper light so that they are clearly readable and identifiable.

K. All the entries in the CAF should be made as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details.

L. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' is to be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF.

M. In case, the customer does not have his/her own mobile number, mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.

N. In any case, the mobile number of authorized officer registered with the Company should not be used for customer signature.

O. It must be verified that mobile number used in customer signature is not mobile number of authorized officer.

P. Authorized officer should provide a declaration about capturing live photograph of customer and original document. For this purpose, authorized official should be verified with OTP sent to the mobile number registered with the Company. This OTP validation is to be treated as authorized officer's signature on the declaration. Live photograph of authorized official should also be captured in the authorized officer's declaration.

Q. Subsequent to all these activities, the KYC Application should give information about the completion of the process and submission of activation request to an activation officer of the Company, and also generate transaction-ID/reference-ID number of the process. Authorized officer should intimate the details regarding transaction-ID/reference-ID number to customer for future reference.

R. Authorized officer of the Company should verify that

i. information available in picture of document is matching with information entered in CAF

ii. live photograph of the customer matches with the photo available in the document

iii. all the necessary details in CAF including mandatory fields are filled properly

S. On Successful verification, the CAF should be digitally signed by authorized officer of the Company and take a print of CAF, should be bear signatures/thumb-impression of customer at appropriate place.

T. The signed document should be scanned and uploaded in system and the original hard copy should be returned to the customer.

Annexure – 3 - Video Based Customer Identification Process (V-CIP)

I. **SCOPE:**

The Company shall undertake V-CIP to carry out the following activities:

- Customer Due Diligence (CDD) in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

  Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm apart from undertaking CDD of the proprietor.
- Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication.
- Updation/Periodic updation of KYC for eligible customers

II. **V-CIP INFRASTRUCTURE:**

While undertaking the V-CIP process, the Company shall ensure that the following infrastructure shall be maintained:

i. The Company shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for financial institutions, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure shall be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Company exclusively owned/ leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud servicer provider or third-party technology provider assisting the V-CIP of the Company.

ii. The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent shall be recorded in an auditable and alteration proof manner.

iii. The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv. The video recordings shall contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber security event under extant regulatory guidelines.

vii. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests shall be carried out periodically in conformance to internal / regulatory guidelines.

viii. The V-CIP application software and relevant APIs / webservices shall undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

III. **V-CIP Procedure:**

A. Live V-CIP should be carried out by an official of the Company after obtaining customer's informed consent.

B. The authorised 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 Digi Locker;

C. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the XML file or QR code generation date should not be older than 3 working days from the date of carrying out V-CIP. Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, 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, if in the rare cases, the entire process cannot be completed at one go or seamlessly;

D. 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;;

E. Clear image of PAN card displayed by customer should be captured, except in cases where e-PAN is provided. PAN details should be verified from the database of Income Tax department including through Digi Locker;

F. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP;

G. 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. 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;

H. Live location of customer (Geotagging) should be captured to ensure that customer is physically present in India;

I. Photograph in Aadhaar/OVD and PAN/e-PAN details should match with the customer and the identification details in Aadhaar/OVD and PAN/e-PAN should match with details provided by customer;

J. Sequence and/or type of questions during video interactions should be varied in order to establish that interactions are real-time and not pre-recorded;

K. Any prompting, observed at end of customer shall lead to rejection of the account opening process;

L. 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 work flow;

M. Video of the customer should be recorded along with photograph;

N. Accounts opened through V-CIP should be operational only after being subjected to concurrent audit;

O. Process should be 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;

P. Liveness check should be carried out in order to guard against spoofing and such other fraudulent manipulations;

Q. To ensure security, robustness and end to end encryption, software and security audit and validation of the V-CIP application should be carried out before rolling it out;

R. Interaction should be triggered from the domain of the Company, and not from third party service provider;

S. Process should be operated by officials specifically trained for this purpose and activity log along with the credentials of the official performing the V-CIP should be preserved;

T. Assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies may be taken, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Company;

Q. Ensure that Aadhaar number is redact or blackout;

U. All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied.

Annexure – 4 – Details of Principal Officer and Designated Director

Designation	Name of Officer
Designated Director	Mr. Nikesh Kumar Sinha, Managing Director
Principal Officer	Ms. Monika Thadeshwar (Variava), Company Secretary & Compliance Officer

Annexure – 5 – AML Screening Mechanism

Particulars	AML Screening (Onboarding)		AML Screening (Annual)	
	Probable Match	Exact Match	Probable Match	Exact Match in Identifier
Match Reported to	1. Head of Operation and 2. National Credit Head	1. Head of Operation; 2. National Credit Head; 3. Chief Risk Officer; and 4. Head of Compliance	1. Head of Operation and 2. National Credit Head	1. Head of Operation; 2. National Credit Head; 3. Chief Risk Officer; and 4. Head of Compliance
Action on Loan Application/Account	Proceed further after evaluation in case of sufficient mitigants or sufficient evidence to disprove match	Reject	Probable match cases will be checked based on the information available in the report	No Further exposure in these cases will be permitted in the form of enhancement or top up. Increase in exposure will not be allowed in existing or any other product.
Steps of Mitigation	Carry out checks on the match attributes such as name, location, gender, address, spouse, family etc. 1. Generic Online checks based on Google search 2. India Kanoon 3. KYC Verification if above both insufficient 4. CPV report based on checks with neighbourhood	None	If it is only a name match with no other matching attributes then it will be considered as a mismatch and will not need further investigations. If there are multiple field matches like name, address, gender, location then it will call for further investigation and mitigants to disprove the match. Further action like the restriction of future funding or reclassification of	None

			KYC risk will be taken on the facts of each case.	
KYC Risk Classification	No reclassification if approved based on sufficient mitigants	High	1. No reclassification if approved based on being inferred as mismatch or having sufficient mitigants to prove mismatch. 2. If mitigants are insufficient, reclassify KYC Risk from Low to Medium or Medium to High as the case may be, in case of a Probable Match in FCRA and SEBI Debarred. 3. If mitigants are insufficient, reclassify KYC Risk from Low to Medium or Medium to High as the	Case to be reclassified as High Risk. For Exact match SEBI debarred cases, to be reclassified as Medium Risk. If it is already at Medium risk it continues at the same risk.

			case may be, in case of a Probable Match in UAPA or UNSC lists.	
Action By Branch Manager	Approval by Branch Manager	N/A	N/A	N/A
Action from Risk	Approval by National Credit Head	N/A	Noting by National Credit Head	Noting by Chief Risk Officer No approval for any other loan or non-loan product or service
Action from Operation	Approval by Head of Operation	N/A	Noting by Head of Operation	Include in quarterly STR (Excluding Sebi debarred exact match)
Action from Compliance	N/A	N/A	Report the results of the Annual/Quarterly AML Screening to Board	Noting by Head of Compliance. Report the results of the Annual/Quarterly AML Screening to Board

***Frequency for bulk AML check post onboarding:** The Company will have Y-O-Y quarterly run of data for AML check and the report will be placed before the Board of Directors for their review and consideration as per the frequency. (AML check done till 31-May-2022, next AML check will be done in July, 2023 (May, 2022 + Cases disbursed In June, 2022), October, 2023 (cases onboarded July-September,2022), January, 2024 (Cases onboarded October-December, 2022) so on and so forth)

x-x-x-x-x-x-x