Policy	Date of Approval:	Next Review: As and when required
KYC and AML Policy (Know Your Customer and Anti Money Laundering Policy)	Effective date of implementation:	Version: V.1.0_04/22

MANGAL
CREDIT & FINCORP LIMITED

Ek mangalmay Shuruvaat

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

Policy	Date of Approval:	Next Review: As and when required
KYC and AML Policy (Know Your Customer and Anti Money Laundering Policy)	Effective date of implementation:	Version: V.1.0_04/22

CONTENTS

Policy	Date of Approval:	Next Review: As and when required
KYC and AML Policy (Know Your Customer and Anti Money Laundering Policy)	Effective date of implementation:	Version: V.1.0_04/22

1. BACKGROUND

The Reserve Bank of India ("RBI") has prescribed Reserve Bank of India (Know Your Customer) Directions, 2016 ("RBI KYC Directions") so that every entity regulated by the RBI complies with the provisions of RBI's Master Directions on KYC (last updated on 10th May 2021) and of PMLA* and the Prevention of Money-Laundering* (Maintenance of Records) Rules, 2005 ("PML Rules"). In accordance with the RBI KYC Directions, Mangal Credit and Fincorp Limited ("MCFL" or "the Company"), being an NBFC, is required to adopt a 'Know Your Customer ("KYC") and Anti-Money Laundering ("AML") Policy'. The Policy as per RBI directions is required to be approved by the Board.

2. POLICY OBJECTIVES AND SCOPE

Key objectives of this KYC and AML Policy("KYC Policy")are as under:

a. To prevent the Company's business channels/products/services from being used as a channel for Money Laundering("ML")/ Terrorist Financing("TF') intentionally or unintentionally.
b. To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Company.
c. To ensure compliance with the applicable laws and regulations from time to time.
d. To protect the Company's reputation.

Scope:

a. KYC and AML Policy guidelines are applicable to all the functions of the organization dealing with customers, vendors / service providers and employees.
b. Functions should adhere to the guidelines mentioned in this policy while drafting their internal policies, procedures, products etc.
c. This policy should be read in conjunction with related operational guidelines issued from time to time by Compliance/Risk, if any.
d.

3. EFFECTIVE DATE

The KYC Policy shall be effective from the date of approval of this policy and supersede previous versions of all policies relating KYC and AML.

4. REVIEW OF POLICY

The KYC Policy shall be reviewed as and when required by the applicable rules and regulations. Such review will be approved by the Board of Directors or the authority to whom the Board may delegate its powers.

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

5. DEFINITIONS

✓ Aadhaar number

Aadhar number means an identification number issued to an individual under sub-section (3) of Section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of Section 3.

✓ Aadhaar Act

Aadhaar Act means Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016

✓ 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 (means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company) or who exercise control (right to appoint majority of the directors or to control the management or policy decisions) through other means.
b. In case of a partnership firm, the BO 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 capital or profits of the partnership.

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.

c. In case of an unincorporated association or body of individuals, the BO 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 entity
d. In case of a trust, the identification of BO shall include identification of the author of the trust, the trustee, the beneficiaries with 15% 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.

✓ Cash Transaction Report (CTR)

CTR will include the following:

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

✓ Certified Copy of Officially Valid Document (OVD)

Certified Copy of Officially Valid Document (OVD) shall mean comparing the copy of OVD with the original and recording the same on the copy as per the PMLA and PML Rules.

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

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

- ✓ Customer
  Customer - is defined to mean a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person, on whose behalf the person who is engaged in the transaction or activity, is acting

- ✓ Customer Due Diligence (CDD)
  Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner.

- ✓ Customer Identification
  Customer Identification means undertaking the process of CDD/Customer identification.

- ✓ Designated Director
  Designated Director means the Managing Director or a whole-time Director designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the Rules.

- ✓ Digital KYC
  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 PMLA.

- ✓ Digital Signature
  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).

- ✓ Equivalent E-Document
  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 client as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

✓ Non-Face-To-Face Customers
Customers who open accounts without visiting the branch/ offices of the Company or meeting its officials.

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

✓ Offline Verification
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.

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

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

✓ Politically Exposed Persons (PEPs)
Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of stateowned corporations, important political party officials, etc.

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

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

a. gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no economic rationale or bona fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

✓ Transactions

means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes

a. Opening of an account.
b. Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means.
c. Entering into any fiduciary relationship.
d. Any payment made or received in whole or in part of any contractual or other legal obligation;
e. Establishing or creating a legal person or legal arrangement.
f. The use of a safety deposit box or any other form of safe deposit & lockers.

✓ 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 Customer Due Diligence (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 CIP for the purpose of this Policy.

6. POLICY STANDARDS

Key Policy standards among others covered in this policy are Customer Acceptance Criteria, Risk Management and Risk categorization from KYC and ML perspective, Customer Identification procedure, monitoring of transaction and account from KYC/ML perspective.

7. CUSTOMER ACCEPTANCE POLICY (CAP) AND CUSTOMER DUE DILIGENCE

For the Customer Acceptance following criteria should be followed:

a. No account should be opened in anonymous or fictitious/benami name(s) and accept customers only after verifying their identity, as laid down in Customer Identification Procedures.
b. Parameters of risk perception should be defined in terms of customer identity, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status. Customer should be categorized as low, medium and high risk. The organization should seek only such information from the customer, which is relevant to the risk category and is not intrusive.
c. Documentation requirements and other information should 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 and guidelines issued by Reserve Bank from time to time.

d. Not to open an account where the organization is unable to apply appropriate customer due diligence measures. i.e. the organization 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.
e. Optional or additional information will be obtained with an explicit consent of the customer.
f. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.
g. Necessary checks should be conducted in CIBIL / Credit Information Company, any notified list of RBI or any other Regulator before accepting the customer and 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.
h. The existing customers and new employees during hiring would be screened against the consolidated list of individuals and banned entities circulated by RBI to ensure that there are no matches.
i. All the customers would be screened through Sanctions list of Office of Foreign Assets Control (OFAC) of US Department of Treasury at the time of on-boarding.
j. Customer profile should be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes within the Company without the express permission of the customer.
k. For sharing the customer information obtained from UIDAI, for sharing the same with other entities, specific permission from UIDAI should be obtained.
l. The above Customer Acceptance Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.
m. The Company may rely on third party verification subject to the conditions prescribed by the RBI, the PMLA and the Rules thereunder in this regard.
n. 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.

Appropriate Enhanced Due Diligence ("EDD") measures shall be adopted for high risk customers from AML perspective. In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures may be adopted. Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at PO level, after giving due notice to the customer explaining the reasons for such a decision.

8. RISK MANAGEMENT

The Company will ensure that it has an effective and appropriate KYC procedures. The overall KYC/ AML program will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibilities will be explicitly allocated within the Company to ensure that the Company's policies and procedures are implemented effectively.

8.A. Concurrent/Internal Audit: To provide reasonable assurance that its KYC and AML procedures are functioning effectively, an audit of its KYC and AML processes will be covered under the Internal/concurrent Audit of the Company as may be applicable on MCFL. The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

8.B. ML & TF Risk Assessment: The Company, as an NBFC, is required to carry out Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise periodically to identify, assess and take effective measures to mitigate these risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. As such, the ML and TF risks for the Company are like to be low as it does not operate in other countries and geographies, its customer base is mainly Indian National only, company is a NBFC hence can't offer liability products like Saving/Current/check in account etc, company offers loans / credit facility with defined end use. The ML and TF Risk Assessment should involve the relevant functions and should have the following stages: Identification, analysis and evaluation. The Company shall conduct the ML and TF Risk Assessment as and when required. The outcome of the ML and TF Risk Assessment should be put up before the Risk Management Committee.

8.C. Risk Categorization: The Company will categorize its customers, based on the assessment, profiling and perceived ML risk, as per the regulatory guidance in this regard. The parameters such as customer's identity, social/ financial status, nature of business activity, and information about the clients' business etc. may also be considered in this regard. Further, the Company will put in place a system of periodical review of risk categorization of accounts in accordance with the regulatory requirements.

8.D. Periodic Updation: The Company will conduct periodic updation of KYC documents at least once in every 2 years for high risk customers, once in every 8 years for medium risk customers and once in every 10 years for low risk customers. Physical presence of such clients is not insisted upon at time of periodic updations. Furthermore, in case of low risk customers, the company may not seek fresh proofs of identity and address at time of periodic updation, in case of no change in status with respect to their identities and addresses. A self-certification by a low risk customer to this effect would be taken as sufficient. In case of change of current address of such low risk customers, the organization should seek a certified copy of the document (proof of address) by mail/post/any other acceptable mode etc.

a. Individual Customers:
   i) No change in KYC information: In case of no change in the KYC information, a self declaration from the customer in this regard to be obtained through customer's email-ID, customer's mobile number registered with us, Mobile application, Letter or any other acceptable mode etc.

ii) Change in address: A copy of OVD or deemed OVD or equivalent e-documents as per KYC Policy for the new address to be obtained from the customer through customer's email-ID, customer's mobile number registered with us , Mobile application and Letter or any other acceptable mode etc.

b. Customers other than individuals:
   i) No change in KYC information: In case of no change in the KYC information of the LE customer, a self-declaration to be obtained from the LE customer through its email ID registered, mobile application, letter from an official authorized by the LE in this regard, board resolution etc. Beneficial Ownership (BO) information available to be reviewed and updated.
   ii) Change in KYC information: To undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

c. Additional measures:
   i) If the validity of the CDD documents available with us has expired at the time of periodic updation of KYC, KYC process equivalent to that applicable for on-boarding a new customer to be undertaken.
   ii) Customer's PAN details, if available, to be verified from the database of the issuing authority at the time of periodic updation of KYC.
   iii) An acknowledgment is to 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.
   iv) If an existing KYC compliant customer desires to open another account with the organization, there may be no need for submission of fresh proof of identity and/or proof of address for the purpose.

8.E. Employee Training - There should be ongoing employee training program so that the staff is adequately trained in KYC Policy and procedures. As the employees' roles could undergo change, all the employees, as applicable / required by RBI/regulations, (including frontline staff, compliance staff and staff dealing with new customers), will undergo training covering all aspects of KYC Policy including empowering them to handle issues arising from lack of customer education.

9. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

The company should identify the customer and verifying his/ her identity by using reliable independent sources of documents, data or information to ensure that the customer is not a fictitious person. Besides risk perception, the nature of information / documents required would also depend on the type of customer (individual, corporate etc.). The CIP is done when starting a account based relationship with a customer, doubt about authenticity / identification of customer, selling third party products, selling own or 3rd party product of fifty thousand or more, transaction involving fifty thousand or more (single or group or series) for non account based customer. Customer due diligence / Identification as under, would be required to be obtained following information / documentation in respect of different classes of customers:

a. Customers that are natural persons:
   i. Address/location details & proof

ii. Identity Proof and
iii. Recent photograph

b. Customers that are legal persons:

i. Legal status of the legal person/entity through proper and relevant documents.
ii. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person is established and verified.
iii. Understand the ownership and control structure of the customer and determine who are the natural persons and ultimately control the legal person.

9.1. Individual Customers (Mandatory Pan Number) – submit following document/e-document

a. The customers would submit OVD for identity and address.
b. Individual customers have to mandatorily submit the Permanent Account Number or Form No. 60. This would also apply to individuals who are beneficial owner, authorized signatory or power of attorney holder related to any legal entity.
c. Recent photograph.
d. Other document including in respect of the nature of business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company

9.1.A. Simplified procedure for opening accounts of Individuals - In case a person who desires to open an account is not able to produce any of the OVDs, the Company may at its discretion open accounts subject to the following:

a. Obtain a self-attested photograph from the customer.
b. The authorized officer of the Company should certify 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 12 months, within which CDD as prescribed above should be carried out.
d. Balance in all account of such a customer together should not exceed Rs.50,000/- at any point of time and maximum credit should not exceed Rs.1Lakh in a year. No transaction will be permitted until full KYC procedure is completed if these limit are breached and same is informed to customer.

9.2. Sole Proprietorship Firms

Documents/e-documents which could be obtained as proof of business/activity for proprietary firms (any two), in addition to the documents of the proprietor as individual:

i. Registration Certificate
ii. Certificate/ license issued by the Municipal authorities under Shop & Establishment Act,
iii. Sales and Income tax returns,
iv. CST / VAT/GST certificate (Provisional/Final)

v. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities
vi. IEC (Importer Exporter Code) issued to the proprietary concern by the office of Director General of Foreign Trade (DGFT)
vii. License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statue
viii. 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
ix. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

In case customer is not able to furnish two documents, the company subject to its satisfaction, collection of other information and verification may accept only one of these documents.

9.3. Partnership Firms:

Where the customer is a partnership firm, the certified copies of the following documents/e-document should be obtained:

i. PAN of the partnership firm
ii. Certificate of registration as available
iii. Partnership deed.
iv. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf. PAN or Form 60 of the persons holding an attorney to transact on its behalf along with any OVD for identity and address proof and one recent photograph of such persons.

9.4. Trusts

Where the customer is a trust firm, the certified copies of the following documents / e-documents should be obtained:

i. PAN/Form No. 60 of the entity
ii. Certificate of registration
iii. Trust deed.
iv. Power of Attorney granted to a member or an employee of the firm to transact business on its behalf. PAN or Form 60 of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons.

9.5 Unincorporated Bodies

Where the customer is an unincorporated association or a body of individuals, the certified copies of the following documents/E-documents should be obtained:

i. PAN/Form No. 60 of the entity
ii. Resolution of the managing body of such association or body of individuals;
iii. Power of attorney granted to him to transact on its behalf. PAN or Form 60 of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons.

9.6 Companies:

Where the customer is a Company, the certified copies of the following documents / E-documents should be obtained:

i. PAN of the Company
ii. Certificate of incorporation
iii. Memorandum and Articles of Association
iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with their PAN or Form 60 and any OVD or Aadhaar card for identity and address proof and one recent photograph of such persons.

9.7 For opening accounts of juridical persons not specifically covered above, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following document / E-documents should be obtained:

i. Document showing name of the person authorized to act on behalf of the entity;
ii. OVD for proof of identity and address in respect of the person holding an Power of attorney to transact on its behalf and one recent photograph.
iii. Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

9.8 Simplified norms for Self Help Groups (SHGs)

i. CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
ii. CDD of all the office bearers shall suffice.
iii. No separate CDD as per the CDD procedure mentioned above of the members or office bearers shall be necessary at the time of credit linking of SHGs.

10. BENEFICIAL OWNERSHIP

For opening an account of an entity who is not a natural person, the beneficial owner(s) (as defined above) shall be identified and all reasonable steps to verify his/her identity shall be undertaken. While doing so, the Company will keep the following in view:

a. Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
b. In cases of trust/ nominee or fiduciary accounts, where it is determined that the customer is acting on behalf of another person as trustee/ nominee or so, identity of the intermediaries and of the persons on whose behalf he is acting, as also details of the nature of the trust or other arrangements in place will be obtained.

There are certain indicative guidelines issued by RBI from time to time for customer identification requirements with regard to matters, such as Trust / Nominee or Fiduciary Accounts, Accounts

of companies & firms, Client Accounts opened by professional intermediaries, Accounts of Politically Exposed Persons resident outside India and Accounts of non-face-to-face customers and these guidelines should be adhered to the extent applicable.

11. UNIQUE CUSTOMER IDENTIFICATION CODE (UCIC)

Every customer should be provided with a unique customer identification code. This will help to identify customers, track the facilities availed, monitor financial transactions and enable the organization to have a better approach to risk profiling of customers.

12. CUSTOMER DUE DILIGENCE

For undertaking CDD, either of the following should be obtained from an individual or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

S No	Nature of the Document	Type of Verification
1	Proof of possession of Aadhaar number where offline verification can be carried out	Offline verification
2	Proof of possession of Aadhaar number where offline verification cannot be carried out	Digital KYC - Annex – I
3	Any OVD containing the details of identity and address	Digital KYC - Annex – I
4	Any equivalent e-document of any OVD containing the details of identity and address	Verification of Digital signature and Live photo - Annex – I

Note :

1. For the purpose of this policy, 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.
2. Aadhaar Offline Verification- The Company may carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purpose. However, where its customer submits his Aadhaar number, the Company will ensure such customer to mask or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar Act.
3. Authentication using e-KYC authentication facility provided by the UIDAI- As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI, it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the PMLA/ the Aadhaar Act/ the RBI KYC Directions.
4. The Company may also carry-out KYC verification under Digital KYC Process defined in Annexure 1.
5. The company may also carry out live Video CIP via its employee after obtaining informed consent from customer with adherence to stipulations as per Annex - II as per Annex II.
6. In case the CDD is outsourced to third party, then the records or the information of the customer due diligence carried out by the third party should be obtained within two days from the third party or from the Central KYC Records Registry. In such cases, decision-making

functions of determining compliance with KYC norms should not be outsourced. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

13. RECORD RETENTION

Records pertaining to identification of the customer and his address obtained while opening his account and during course of business relationship should be preserved for at least five years after the business relationship has ended. All necessary records of transactions of the customer, both domestic and international, should be maintained for at least five years from the date of transaction.

14. ENHANCED DUE DILIGENCE PROCEDURE

14.1 Accounts of Politically Exposed Persons (PEPs):

Politically exposed persons are individuals, who are or have been entrusted with prominent public functions e.g. heads of states or of governments, senior politicians, senior government / judicial / military officers, senior executives of state owned corporations, important political party officials etc.

Decision to deal with such persons as a customer shall be taken up at a senior management level and should be subjected to enhanced monitoring. The norms are also applied to the accounts of the family members or close relatives of PEPs.

In case of an existing customer or beneficial owner of an existing account subsequently becoming PEP, matter should be reported to senior management level and be subjected to enhanced monitoring. The above will also be applicable to accounts where a PEP is the beneficial owner.

14.2. Accounts of non-face-to-face customers:

In the case of non-face-to-face customers, it should be ensured that the first payment is effected through the customer's KYC-complied account with another regulated entity.

15. CENTRAL KYC REGISTRY (CKYC)

The Company, as applicable to it, will capture the KYC information/ details as the KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records could be retrieved online from CKYCR and customer is not required to submit any KYC records unless

a. there is a change in information of customer as existing in the records of CKYCR;

b. current address of customer is required to be verified;

c. it is considered necessary to verify identity or address of customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

KYC Identifier generated by CKYCR, should be communicated to the Individual/LE.

16. MONITORING OF TRANSACTIONS

The organizations monitoring activity should depend on the risk sensitivity of the account and high value cash transactions. High risk accounts should be subjected to intensified monitoring.

All transactions including those of suspicious nature like "a customer who is reluctant to provide information needed for a mandatory report, an account where there are several cash transactions below a specified threshold level to avoid filing of reports, employee whose lavish lifestyle cannot be supported by his or her salary, negligence of employee / willful blindness is reported repeatedly " etc. should be reported to the Compliance Head on a monthly basis.

Cash Transaction Report (CTR), as applicable to company, in respect of cash transactions of INR 1 Million and above undertaken in an account either single or in an integrally connected manner in a calendar month should be reported to FIU – IND by 15th of the succeeding month or as required by FIU.

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

Suspicious Transaction Report (STRs) may, as applicable to company, be reported 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. A customer whose transaction is reported as Suspicious to FIU should be treated as "high risk" customer for a period of one year from the date of reporting.

The organization should maintain proper records of series of cash transactions of a customer below Rs. 1 Million but monthly aggregate exceeding Rs. 1 Million and the records related to transactions reported as suspicious transactions to FIU – India. These records should be retained for a period of five years from the date of transaction.

The organization should put in place a system of periodic review (at least once in 12 months) of risk categorization of accounts and need for applying enhanced due diligence measures.

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

17. CUSTOMER EDUCATION

The organization may prepare specific literature / pamphlets etc., to educate the customer of the objectives of the KYC program. The frontline lending and operating managers should be fully equipped with the compliance requirements of KYC guidelines in respect of new customer acquisition and shall adhere to the Customer Identification & Acceptance procedure.

18. KYC FOR THE EXISTING ACCOUNTS

KYC norms are applicable to all the existing customers in a time bound manner. Where the organization is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the debit operations may be stopped.

19. SELLING OF THIRD PARTY PRODUCTS

The Company, if acting as agents while selling third party products as per regulations in force from time to time, will comply with the following aspects:

(a) The identity and address of the walk-in customer shall be verified for the transactions as required under the CIP prescribed above;

(b) Transaction details of sale of third-party products and related records shall be maintained.

(c) Monitoring of transactions for any suspicious activity will be done.

20. ADHERENCE TO KNOW YOUR CUSTOMER (KYC) GUIDELINES BY THE COMPANY'S AGENTS

(a) The Company's agents or persons authorized by it, for the its business, will be required to be compliant with the AML/ KYC Policy applicable to the Company.

(b) All information shall be made available to the RBI to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorized by the Company including agents etc. who are operating on its behalf

21. PRINCIPAL OFFICER AND DESIGNATED OFFICER

(a) Designated Director- The Company will nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules thereunder.

(b) Principal Officer- The Company designate one of its senior officials as the 'Principal Officer' who will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

22. REVIEW OF THE POLICY

This Policy should be reviewed if there are any amendments in the regulatory guidelines and the such amendments and revision in policy may be done after approval from the Designated Director based on the recommendation of the Principal Officer. Further, the Designated Director, based on recommendation from the Principal Officer, will have authority to approve various Processes to implement the KYC Policy. The policy will be reviewed by board as and when required or in year when any material changes in policies are carried out.

ANNEX -I DIGITAL KYC PROCESS

A. A Digital KYC Application (KYC App) 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 App 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 App 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 App 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 Application form or other documents.
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 Application form.
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 App 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 the 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.

ANNEX - II DIGITAL KYC PROCESS

VIDEO CUSTOMER IDENTIFICATION PROCESS (V-CIP)

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

B. Video of the customer should be recorded along with photograph

C. For identification of the customer, offline verification of Aadhaar should be conducted

D. 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 Income Tax department.

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

F. Photograph in Aadhaar/PAN details should match with the customer and the identification details in Aadhaar/PAN should match with details provided by customer.

G. 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.

H. 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 days from the date of carrying out V-CIP.

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

J. 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.

K. Liveliness check should be carried out in order to guard against spoofing and such other fraudulent manipulations.

L. 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.

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

N. 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.

O. Video recording should be stored in a safe and secure manner and bear the date and time Stamp.

P. 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.

V-CIP INFRASTRUCTURE

(i) Comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

(ii) 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 should be recorded in an auditable and alteration proof manner.

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

(iv) The video recordings should 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, even though the ultimate responsibility of any customer identification rests with the RE. 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 suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / web services shall also 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.

V-CIP PROCEDURE

(i) Organization shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Organization specially trained for this purpose. The official should be capable to carry out

liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

(iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

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

(v) 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.

(vi) The authorized official of the Organization 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:

a) KYC records downloaded from CKYCR, in accordance with Master direction, using the KYC identifier provided by the customer

b) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker Organization shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of Master Direction. 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 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, Organization shall ensure that the video process of the V-CIP is undertaken within three 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. Further; Organization shall ensure that no incremental risk is added due to this.

(vii) 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.

(ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

V-CIP RECORDS AND DATA MANAGEMENT

(i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Organization 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 extant instructions on record management, as stipulated in this RBI Master Direction, shall also be applicable for V-CIP.

(ii) The activity log along with the credentials of the Organization official performing the V-CIP shall be preserved

Policy	Date of Approval:	Next Review: As and when required
KYC and AML Policy (Know Your Customer and Anti Money Laundering Policy)	Effective date of implementation:	Version: V.1.0_04/22

GLOSSARY

RBI - Reserve Bank of India
CAP - Customer Acceptance Policy
CIP - Customer Identification Procedures
PMLA - Prevention of Money Laundering Act
PEP - Politically Exposed Person
KYC - Know Your Customer
AML - Anti-Money Laundering
NBFC - Non-Banking Financial Companies
CTR - Cash Transaction Report
STR - Suspicious Transaction Report
FIU - Financial Intelligence Unit – India
CIBIL - Credit Information Bureau (India) Limited
UIDAI - Unique Identification Authority of India
OVD - Officially Valid Document
CERSAI - Central Registry of Securitization Asset Reconstruction and Security Interest
CDD - Customer Due Diligence
NRI - Non Resident Indian
PIO - Person of Indian Origin
V-CIP Video based Customer Identification Process
LE Legal Entity

Policy	Date of Approval:	Next Review: As and when required
KYC and AML Policy (Know Your Customer and Anti Money Laundering Policy)	Effective date of implementation:	Version: V.1.0_04/22