KNOW YOUR CUSTOMER

AND

ANTI MONEY LAUNDERING POLICY (V3.1)

Created pursuant to the Reserve Bank of India (Non-Banking Financial Companies -Know Your Customer (KYC)) Directions, 2025 and amended from time to time & approved by the Board on 25-Sept-2026



Table of Contents

1. Purpose and Scope 4

2. Compliance with the Policy 5

3. Customer Acceptance Policy 5

4. Guidelines for Accepting Customers 7

5. Risk Level Categorization 9

6. Customer Data Confidentiality 11

7. Customer Identification Procedure (CIP) 12

8. Customer Due Diligence (CDD) Procedure 14

9. Monitoring of Transactions and Maintenance of Transaction Records 21

9.1 Ongoing due diligence 22

9.3 Maintenance of Records of Transactions 25

10. Requirements and Obligations under International Agreements and Communications from International Agencies 26

11. Risk Management 27

12. General 28

12.1 Appointment of Designated Director 28

12.2 Appointment of Principal Officer and reporting to Financial Intelligence Unit - India 28

12.3 Hiring of Employees and Training 29

12.4 Sharing KYC Information with Central KYC Records Registry 30

12.5 Identification of Beneficial Owner: 31

12.6 Group-Wide Policy 32

12.7 Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010: 32

12.8 Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards: 32

12.9 Allocation of Authorities and Responsibility 33

12.10 Operation of accounts and Money Mules 36

12.11 New Products Launch 36

12.12 Wire transfer / Fund Transfers Related to Lending Operations 37

12.13 Third Party Products 37

ANNEXURE I 38

Digital KYC Process 38

ANNEXURE II 42

V-CIP Process 42

1. Purpose and Scope

1. The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure compliance with the Prevention of Money Laundering Act (PMLA), 2002, as amended from time to time ("**Act**"), and the rules framed thereunder ("**Rules**") and the guidelines issued by the Reserve Bank of India (RBI) under its Master Direction on Non-Banking Financial Companies – Know Your Customer, 2025, dated November 28, 2025 having reference no. RBI/DOR/2025-26/361 and amendments thereafter ("**Master Direction**") and put in place with the approval of the board of directors of the Company (*defined below*) ("**Board**") a policy on Know Your Customer and Anti Money Laundering.

2. 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 **Kaleidofin Capital Private Limited** ("**the Company**") to manage its risks prudently.

3. Accordingly, the main objective of this Know Your Customer and Anti Money Laundering Policy (this "**Policy**") is to enable the Company to ensure proper identification of its customers.

4. This policy is applicable to all categories of products and services offered by the Company. The scope of the Policy is:
    - To lay down explicit criteria for acceptance of customers.
    - To establish procedures to identify 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.

    To fulfil the scope, the following key elements have been incorporated in the Policy:
    - Customer Acceptance Policy
    - Customer Identification Procedures (CIP)
    - Customer Due Diligence (CDD) Procedures
    - Monitoring of Transactions
    - Risk Management
    - Record Management

Capitalized terms used in this Policy but not specifically defined herein shall have the meaning ascribed to them under the Master Direction.

2. Compliance with the Policy

1. Compliance, Credit Risk & Operations department(s) of the Company is entrusted with the responsibility to ensure that the compliance with this Policy is being checked in the internal process audits conducted on the Company. The decision-making functions of determining the compliance of KYC norms are not be outsourced by the Company.

2. All the procedures identified in this Policy are to be carried out for all the business verticals of the Company.

3. Compliance, Credit Risk & Operations department(s) of the Company is entrusted with the responsibility to ensure that Company always remains in compliance of all the requirements and mandates of the Act, Rules and the direction provided by RBI under the Master Directions, as amended or updated, from time to time.

3. Customer Acceptance Policy

1. Definitions

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

'**Person**' shall have the meaning assigned to the same under the Act and shall include:

a. an Individual;
b. a Hindu Undivided Family;
c. a Company;
d. an association of persons or a body of individuals, whether incorporated or not;
e. every artificial juridical person, not falling within any one of the above person (a to d);
f. any agency, office or branch owned or controlled by any one of the above persons (a to e)

'**Beneficial Owner'** (BO) - in relation to a Customer, is a person or an entity who is to be considered a beneficiary of the financial transaction entered in to with the Company by the Customer. A list of persons who are to be considered as such BOs in relation to a Customer is given below:

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

Explanation- For the purpose of this sub-clause

1. **"Controlling ownership interest"** means ownership of/entitlement to more than 10 percent 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) In case where the customer is a **partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation: For the purpose of this sub-clause, '**control**' shall include the right to control the management or policy decision.

c) In case where the customer is a unincorporated association or body of individuals or societies, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent 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) In case where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent 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.

'**Kaleidofin Group'** or **'Group'** shall have the meaning assigned to the term "group" under clause (e) of sub-section (9) of Section 286 of the Income-tax Act, 1961, as amended, modified or re-enacted from time to time.

For the avoidance of doubt, this Policy applies directly to the Company. References to the Kaleidofin Group or Group in this Policy shall apply only in relation to the Company's obligations concerning group-wide programmes against money laundering and terrorist financing, including information sharing for customer due diligence and ML/TF risk management, subject to applicable confidentiality, data protection and anti-tipping-off requirements.

'Senior Management' shall mean and include, Managing Director, Chief Executive Officer, Chief Compliance Officer / Head of Compliance, Chief Risk Officer / Head of Risk, Chief Operating Officer / Head of Operations, or any other senior officer specifically authorised by the Board for the purposes of this Policy. Wherever this Policy requires approval of Senior Management, approval by any one of the aforesaid officers shall be sufficient, subject to such officer not being the originator or recommender of the relevant proposal.

'**Video based Customer Identification Process (V-CIP)**': means an alternative method by which an authorised official of the Company can conduct customer identification with facial recognition and customer due diligence. This process involves a 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 which the customer furnished, through independent verification and by maintaining an audit trail of the process and the Company will treat such processes complying with prescribed standards and procedures on par with face to-face CIP.

4. Guidelines for Accepting Customers

The following norms and procedures will be followed by the Company in relation to its customers who approach the Company for availing financial facilities: While taking decision to grant any one or more facilities to customers as well as during the continuation of any loan account of the customer, the following norms will be adhered to by the Company:

1. No loan or other account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account .i.e. Benami Account. The Operations department(s) of the Company while opening the new account with a prospective customer is to ensure and insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.

2. No loan account or other transactions will be opened / undertaken where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

3. Operations & Credit Risk department(s) of the Company is to ensure that no account is opened or give / sanction any loan or close an existing account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:
   - The Company is unable to verify the identity of the customer
   - The customer without any valid or convincing reasons refuses to provide documents to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity
   - Information furnished by the customer does not originate from the reliable sources or appears to be doubtful due to lack of supporting evidence.
   - Identity of the customer, directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.

4. The Credit Risk & Operations departments of the Company are to ensure and apply Customer Due Diligence (CDD) procedure at the Unique Customer Identification Code (UCIC) level. Accordingly, when any existing KYC-compliant customer desires to open another account or avail of any other product or service from the Company, there will be no need for a fresh CDD exercise as far as identification of the customer is concerned.

5. Subject to the above-mentioned norms and caution, at the same time all the employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

6. The Operations Department, at the time of approving a financial transaction/activity, or executing any transaction, is to verify the record of identity, signature proof and proof of current address or addresses including permanent address of the customer.

7. Suitable systems are put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of the Master Directions or circulated by Reserve Bank of India from time to time.

8. Circumstances, in which a customer is permitted to act on behalf of another person /entity, are to 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 may be opened by intermediary in a fiduciary capacity.

9. Where an equivalent e-KYC document is obtained from the customer, the Company's partner and the Operations Department of the Company is to verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and relevant regulations from the Reserve Bank of India in this regard.

10. The Customer Acceptance Policy is intended not to result in denial of a financial facility to members of the general public, especially those who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). Operations department(s) of the Company should not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned is required to duly record the reason(s) for rejection.

11. Where any employee or officer of the Company suspects money laundering or terrorist financing and reasonably believes that performing the CDD process may tip off the customer, such employee or officer shall not pursue the CDD process and shall promptly escalate the matter to the Compliance Department or the Principal Officer. The Principal Officer shall evaluate the matter and, where appropriate, file an STR with FIU-IND in accordance with applicable requirements. The customer shall not be informed of such escalation or filing.

5. Risk Level Categorization

1. The Credit Risk department of the Company should adopt a Risk Based Approach (RBA) for mitigation and management of the risks and it should categorize its customers based on the risk perceived by the Company. The levels of categorization of risk would be Low, Medium and High. The risk categorization would be a function of different factors including the asset class, the industry the borrower operates in, the geography in which the borrower operates, conditions stipulated in national risk assessment, etc.

   Risk Categorization of the onboarded customers may take into consideration the Proof of Identity, Proof of Address, PEP status, Occupancy status and such other factors as may be deemed necessary from time to time basis the customer profile

2. Risk levels will be decided based on risk element involved in each case which will be determined by considering the following information submitted by the customer:
   - Nature of business of the Customer and of his Clients
   - Work place of Customers and of his Clients
   - Country of Origin
   - Source of funds

- Volume of business six-monthly / annual turn-over
- Social/Legal and financial status
- Quantum and tenure of facility and end-use of the loan

3. Information to be collected from the customers will vary according to categorization of customer from the point of view of risk perceived. However, while preparing customer profile the Company should seek only such information from the customer which is relevant to the risk category and is not intrusive to the customer. Any other information from the customer should be sought separately with his/her consent and after opening the account.

4. For risk categorization, individual (other than High Net Worth) and entities whose sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile, may be categorized as low risk or Level-I category.

5. Self-employed individuals, however with regular income and good credit behaviour Cases where the Company is likely to incur higher than average risk will be categorized as medium or high-risk customers and will be placed in medium or high risk category i.e. Level-II or Level-III category.

6. Politically Exposed Persons ("PEPs") are individuals who are or have been entrusted with prominent public functions by a foreign country, including heads of State or Government, senior politicians, senior government, judicial or military officers, senior executives of state-owned corporations and important political party officials. The applicable requirements shall also extend to their family members and close associates.

   The Company shall apply appropriate risk management measures to identify PEPs and shall obtain approval from Senior Management before establishing, or continuing, a business relationship with a PEP. Such relationships shall be subject to appropriate due diligence, including reasonable measures to establish the source of funds or wealth, and enhanced ongoing monitoring.

7. Certain customers of the special category (CSC) will also be subject to enhanced due diligence. An indicative and non-exhaustive list of such customers is as below:
   - NRI Customers
   - Trusts (except trusts appropriately set up under a specific regulation)
   - Societies
   - Charitable institutions
   - NGOs and other organizations receiving donations from within or outside the country
   - Partnership firms with sleeping partners
   - Family-owned companies

- Persons with dubious or notorious reputation as per the information available from different sources like media, newspapers etc
- Companies having close family shareholding or beneficial ownership
- High net worth individuals
- Non-face to face customers

Note: The above customer categories do not presently form part of the Company's target customer segment. However, if the Company proposes to onboard or otherwise deal with any such customer, the applicable enhanced due diligence and approval requirements shall be completed before establishing or continuing the relationship.

8. Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment

- The Credit Risk department of the Company should carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercises periodically, i.e. every half year, to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for Customers, countries or geographic areas, products, services, transactions or delivery channels, etc.

- The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, credit risk department of the Company is to take cognizance of the overall sector-specific vulnerabilities, if any, that the regulators may share with Company from time to time.

- The Credit Risk department of the Company is to ensure it regularly conducts and properly document its risk assessment exercise as required considering the nature, size, geographical presence, complexity of activities / structure, etc. of the Company ("**Risk Assessment Exercise**"). Further, the Board or a committee of the Board to which it has delegated power is required to determine the periodicity of the aforesaid Risk Assessment Exercise, considering the outcomes and requirements of the aforesaid Risk Assessment Exercise. Provided that, review of Risk Assessment Exercise and its outcomes should be done at least once in a year.

- Credit Risk and Compliance department(s) of the Company is to present the outcome of the exercise to the Board or any committee of the Board to which the Board has delegated power in this regard. The outcome is to be made available to competent authorities and self-regulating bodies.

6. Customer Data Confidentiality

For the purpose of preparing customer profile only such relevant information from the customers

will be sought based on which the Company can easily decide about the risk category in which the customers are to be placed. Ordinarily, the customer profile maintained by the Company will be kept confidential except for cases where the customer himself allows and/or gives consent for the use of the information given in customer profile / application form for offering other products / services of other companies / entities belonging to the Company's group or any other legal entity with whom the Company is having any business tie-ups. However, while taking any such permission or consent of the customer for using his above referred information provided to the Company, it will be ensured that such permission / consent of the customer is unambiguous and explicit.

7. Customer Identification Procedure (CIP)

1. Operations department of the Company is to undertake identification of the customers in the following cases, as applicable:

    a) Commencement of an account-based relationship with the customer.
    b) Carrying out any international money transfer operations for a person who is not an account holder of the Company.
    c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
    d) Selling third-party products, if applicable as agents, selling its own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than ₹50,000.
    e) Carrying out transactions for a non-account-based customer, i.e., a walk-in customer, where the amount involved is equal to or exceeds ₹50,000 whether conducted as a single transaction or several transactions that appear to be connected.
    f) When Credit Risk department of the Company has reason to believe that a customer (account-based or walk in) is intentionally structuring a transaction into a series of transactions below the threshold of ₹50,000.

2. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship or while carrying out an occasional transaction of an amount equal to or exceeding ₹50,000 whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, the Company, at its option, may rely on customer due diligence done by a third party, subject to the following conditions:

    a) The Company obtains the records or information of the customer due diligence carried out by the third party immediately from the third party or from the Central KYC Records Registry.
    b) The Company is to take adequate steps to satisfy itself that the third party will make

copies of identification data and other relevant documentation relating to the customer due diligence requirements available, upon request, without delay.

c) A regulator regulates, supervises, or monitors the third party, and the third party has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Act.

d) The Company is to ensure that the third party is not based in a country or jurisdiction assessed as high-risk.

e) The Company will have the ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable.

3. The Company shall from time to time decide on 1) customer due diligence (CDD) procedures, 2) documents to be collected and stored and 3) KYC processes in accordance with the type of customer and nature of transaction / engagement / relationship with the Company. In accordance with regulations from the Reserve Bank of India in this regard, the customer identification procedure to include the following as applicable:

- Establishing proof of identity (PoI)
- Establishing proof of address (PoA)
- Photograph (where applicable)
- Verification of business constitution documents (where applicable)
- Verification of business registration documents;
- RE-to-RE KYC
    - The Company may also rely on customer due diligence by third parties (subject to customer consent) that are Regulated Entities ("**REs**") as defined by the Reserve Bank of India from time to time. In such cases, copies of the Officially Valid Documents (OVDs) should be provided by the REs and these documents should be further verified by the Operations Department of the Company. Alternatively, the Company may rely on Central KYC records as per information provided by the RE or the customer.

- Aadhaar-based e-KYC
    - The Company may carry out Aadhaar-based e-KYC, either with OTP authorization or with biometric authorization as per extant guidelines from the Reserve Bank of India and from the Unique Identification Authority of India (UIDAI)
- Digital KYC (in accordance with extant guidelines from RBI in this regard); or
- Video-KYC (in accordance with extant guidelines from RBI in this regard) (where applicable)

Provisions under Prevention of Money Laundering Act (PMLA)

1. As per the provisions of 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), Operations & Credit Risk department of the Company is to ensure that:

   - 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
   - In all other cases, verify identify while carrying out:
     - 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,
     - Any international money transfer operations.

   In terms of proviso to Rule 9 of the PML Rules, the relaxation, in verifying the identity of the client within a reasonable time after opening the account / execution of the transaction, stands withdrawn.

   Abiding by the provisions of Rule 9 of the PML Rules, the Operations & Credit Risk department of the Company is to identify the beneficial owner and take all reasonable steps to verify his identity. The said PML Rule also require that the Company should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

   Customer identification requirements are to be aligned as per the provisions of the said rule.

8. Customer Due Diligence (CDD) Procedure

1. CDD Procedure in case of Individuals:

   a) Operations department of the Company should obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

      i. the **Aadhaar number** where:
         a. they are 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

b. they decide to submit their Aadhaar number voluntarily to the Company; or

ii. the **proof of possession of Aadhaar number** where the Company can carry out offline verification; or

iii. the **proof of possession of Aadhaar number where the Company cannot carry out the offline verification** or any OVD or the equivalent e-document thereof containing the details of their identity and address; or

iv. the **KYC Identifier** with an explicit consent to download records from CKYCR; and

v. the **PAN** or **the equivalent e-document** thereof or Form No. 97 as defined in Income-tax Rules, 1962; and

vi. Credit Risk department of the Company may require such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof.

Provided that, where the customer has submitted,

(i) Aadhaar number, the Operations department] of the Company to carry out authentication of the customer's Aadhaar number using UIDAI's e-KYC authentication. Further, in such a case, if the customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, they may give a self-declaration to that effect to the Company.

(ii) an equivalent e-document of any OVD, the Operations department of the Company is to verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a live photo as specified under **Annexure I** of this Policy.

(iii) any OVD or proof of possession of Aadhaar number where offline verification cannot be carried out, the Operations Department of the Company is to carry out verification through digital KYC as specified under **Annexure I of this Policy**.

(iv) Where a KYC Identifier is provided or available, the Company shall retrieve the KYC records online from the CKYCR in accordance with **Para no. 12.4 of this Policy** Direction.

Provided that

(a) where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required.

(b) The Company can perform biometric-based e-KYC authentication, including Aadhaar Face Authentication.

(c) The Company to ensure that the use of Aadhaar, proof of possession of Aadhaar etc., is in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

(d) Aadhaar number is not mandatory for purposes of KYC. However, in case the customer 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), in such case, the customer is to provide the Aadhaar number to the Company. In other cases, customers may provide the Aadhaar number voluntarily.

b) The Company to follow the CDD procedure for all the joint account holders individually, while opening a joint account, or co-borrower account.

2. CDD Measures for Sole Proprietary firms

a) For opening an account in the name of a sole proprietary firm, the Company is to carry out the CDD of the individual (proprietor).

b) In addition to the above, the Company shall also obtain any two of the following documents or the equivalent e-documents thereof as proof of business / activity in the name of the proprietary firm:

i. Registration certificate including Udyam Registration Certificate (URC) issued by the Government;
ii. Certificate / licence issued by the municipal authorities under Shop and

Establishment Act;

iii. Sales and income tax returns;
iv. CST / VAT / GST certificate;
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 DGFT or Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute;
vii. 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; or
viii. Utility bills such as electricity, water, landline telephone bills, etc.

c) In cases where the Credit Risk and Operations department of the Company is satisfied that it is not possible to furnish two such documents, the Company may, at its discretion, accept only one of those documents as proof of business / activity.

Provided that the Company undertakes contact point verification and collects such other information and clarifications as would be required to establish the existence of such firm, and confirm and satisfy itself that it has verified the business activity from the address of the proprietary concern.

3. CDD Measures for Legal Entities

a) For opening an account of a **company**, the Business and Operations department(s) of the Company to obtain certified copies of each of the following documents or the equivalent e-documents thereof:

i. Certificate of incorporation;
ii. Memorandum and Articles of Association;
iii. PAN of the company;
iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
v. Documents relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
vi. The names of the relevant persons holding a senior management position; and
vii. The registered office and the principal place of its business, if it is different.

b) For opening an account of a **Partnership Firm**, the Business and Operations department(s) of the Company to obtain certified copies of each of the following

documents or the equivalent e-documents thereof:

i. Registration certificate
ii. Partnership deed
iii. PAN of the partnership firm
iv. Documents relating to beneficial owner,
v. managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
vi. the names of all the partners and
vii. address of the registered office, and the principal place of its business, if it is different.

c) For opening an account of a **Trust**, the Business and Operations of the Company to obtain certified copies of each of the following documents or the equivalent e-documents thereof:

i. Registration certificate;
ii. Trust deed;
iii. PAN or Form No.60 of the trust;
iv. Documents relating to beneficial owner;
v. managers, officers or employees, as the case may be, holding an attorney to transact on its behalf;
vi. the names of all the beneficiaries, trustees, settlor, protector, if any and authors of the trust;
vii. the address of the registered office of the trust; and
viii. list of trustees and documents for those discharging the role as trustee and authorised to transact on behalf of the trust.

d) For opening an account of an **unincorporated association (includes unregistered trusts / partnership firms) or a body of individuals (includes societies)**, the Business and Operations department of the Company to obtain certified copies of each of the following documents or the equivalent e-documents thereof:

i. Resolution of the managing body of such association or body of individuals;
ii. PAN or Form No. 60 of the unincorporated association or a body of individuals;
iii. Power of attorney granted to transact on its behalf:
iv. Documents relating to beneficial owner;
v. managers, officers or employees, as the case may be, holding an attorney to transact on its behalf; and
vi. Such information as may be required by the Credit Risk department] of Company to collectively establish the legal existence of such an association or body of

individuals.

e) For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, the Business and Operations department of the Company to obtain and verify the certified copies of the following documents or the equivalent e-documents thereof:

i. Document showing name of the person authorised to act on behalf of the entity;
ii. Documents, as specified in paragraph 8(a) of this Policy, of the person holding an attorney to transact on its behalf; and
iii. Such documents as may be required by the Credit Risk department] of Company to establish the legal existence of such an entity / juridical person.

4. Identification of 'Beneficial Owner'

a) For opening an account of a Legal Person who is not a natural person, the Credit Risk department of the Company to identify the beneficial owner(s) and undertake all reasonable steps in terms of sub- rule (3) of Rule 9 PML Rules verify their identity, keeping in view the following:

i. Where the customer or the owner of the controlling interest is;

a. an entity listed on a stock exchange in India;
b. it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions; or
c. it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

ii. In cases of trust / nominee or fiduciary accounts, the Credit Risk department of Company is to determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. In such cases, the Company is to obtain satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place.

5. Enhanced Due Diligence Procedure for non-face-to-face customer onboarding (other than customer onboarding in terms of **Annexure I** of this Policy)

a) Non-face-to-face onboarding facilitates the Company is to establish a relationship

with the Customer without meeting the customer physically, as per **Annexure I** of the Policy or through V-CIP as per **Annexure II** of the Policy. Such non-face-to-face modes to include 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. The Operations and Credit Risk department of the Company is to undertake the following EDD measures for non-face-to-face customer onboarding (other than customer onboarding in terms of **Annexure I** of this Policy):

i. If Company has introduced the process of V-CIP, the Company shall ensure that it provides the same as the first option to the customer for remote onboarding. The Company is to treat processes complying with prescribed standards and procedures for V-CIP on par with face-to-face Customer Identification Process.

ii. In order to prevent frauds, alternate mobile numbers should be avoided and not linked post CDD with such accounts for transaction OTP, transaction updates, etc. The Business and Operations department of the Company to permit transactions only from the mobile number used for account opening.

iii. Apart from obtaining the current address proof, the Company is to ensure and verify the current address through positive confirmation before allowing operations in the account. The Company may carry out the positive confirmation by means such as address verification letter, contact point verification, deliverables, etc.

iv. The Business and Operations department of the Company to ensure and obtain PAN from the customer and the PAN is to be verified from the verification facility of the issuing authority.

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

vi. The Company to ensure categorising such customers as high-risk customers and to ensure that subject accounts be opened in non-face-to-face mode to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP as per **Annexure II** of the Policy.

Note: Currently the Company is not undertaking non-face to face onboarding and V-CIP process. The necessary compliances as applicable for the above shall be followed as and when the respective process is started by the Company.

6. Accounts of Politically Exposed Persons (PEPs):

   a) Company before and during establishing the relationship with Politically Exposed Persons (as a Customer or as beneficial owner), and/or their family members and/or their close associates, apart for maintaining the prudent CDD practices, to ensure that:

      i. Credit risk department of the Company to ensure having an appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

      ii. Credit risk department of the Company to ensure reasonable measures are in place for establishing the source of funds / wealth;

      iii. Business department of the Company to ensure prior approval from the Senior Management for opening an account for a PEP;

      iv. Credit Risk department of the Company subjects all the accounts of PEP to enhanced monitoring on an on-going basis;

      v. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Business department of the Company to ensure obtaining the Senior management's approval to continue the business relationship with such PEP;

7. Accounts opened by professional intermediaries: The Company shall not establish a customer relationship with a professional intermediary acting on behalf of one or more underlying clients unless the identity of each relevant client and beneficial owner can be identified and verified to the satisfaction of the Company.

9. Monitoring of Transactions and Maintenance of Transaction Records

1. The Credit Risk department of the Company is to ensure monitoring of the transactions of a suspicious nature on a continuous basis for the purpose of reporting it to the appropriate authorities. The extent of monitoring by the Company will depend on the risk sensitivity of the account and special attention will be given to all complex unusually large transactions, which have no apparent economic or lawful purpose.

2. The Credit Risk department of the Company is to exercise caution with respect to the transactions with persons (including legal persons and other financial institutions) from the countries which have been identified by Financial Action Task Force (FATF) as high risk and non-cooperative jurisdictions with respect to compliance with the FATF

Recommendations, 2012.

3. The Compliance department of the Company to ensure filing of Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling under FATCA in terms of the direction of the RBI/PMLA in respect of all products/ services.

9.1 Ongoing due diligence

1. The Credit Risk and Finance department of the Company to undertake on going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, and source of funds / wealth.

2. Any unusual pattern in the operations of the accounts like, large and complex transactions including RTGS transactions, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose, transaction exceeding threshold limits, high turnover in the accounts compared to the average outstanding etc. is to be closely monitored. The extent of monitoring should be aligned with the risk category of the Customer and high-risk category accounts should be subjected to more intensified monitoring.

3. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures should be put in place. The Company does not engage or do business with Multi-level Marketing (MLM) companies.

9.2 Periodic updation of KYC

1. As per the Master Direction, the Company has adopted a risk-based approach for periodic updation of KYC in the following manner:

S. No.	Risk category	Frequency
1	**High risk customers**	Once in every two years from the date of opening of the account / last KYC updation
2	**Medium risk customers**	Once in every eight years from the date of opening of the account / last KYC updation
3	**Low risk customers**	Once in every ten years from the date of opening of the account / last KYC updation

In respect of an individual customer categorised as low-risk, the Company shall permit transactions and complete periodic updation of KYC within one year from the date on

which such updation becomes due. The account shall be subject to regular monitoring during such period.

2. Individuals
   a) The Company to obtain self-declaration from Individual customers in case of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained and the declared address be obtained through Customer's email-id, Customer's mobile number, digital channels (including mobile application that may be used by the Company), and be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

   b) The Operations Department of the Company to ensure obtaining a copy of Officially Valid Documents (OVD) or deemed OVD or the equivalent e-documents thereof, as defined in Section 5(1)(a)(xiv) of Master Direction, for the purpose of proof of address, declared by the customer at the time of periodic updation.

   c) In case of change in KYC information, the Operations department(s) of the Company to ensure undertaking a KYC process equivalent to on-boarding a new customer.

   d) The Company does not provide loan to minors.

   e) Operations Department of the Company may use Aadhaar OTP based e-KYC in non-face-to-face mode for updation / periodic updation. Conditions stipulated in **Annexure I** are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

   f) Declaration of current address: where the current address declared by the customer differs from the address recorded in the Aadhaar, the Business and Operations Departments of the Company has to ensure that the mobile number used for Aadhaar authentication is identical to the mobile number recorded in the customer's profile with the Company, so as to mitigate and prevent the risk of fraud.

3. Non-Individuals

   a) No change in KYC information: In case of no change in the KYC information of the 'Legal Entities' ("**LE**") customer, the Credit Risk department of Company is to ensure procuring a self-declaration in this regard from the LE customer through its email id registered with the Company, digital channels (including mobile application), letter from an official authorised by the LE in this regard, board resolution, etc. Further, Credit Risk department(s) of the Company to ensure during this process that Beneficial

Ownership (BO) information available with them is accurate and 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 Credit Risk department of Company is to ensure undertaking the KYC process equivalent to that applicable for onboarding a new LE customer.

4. Additional Measures:

a) Operations department of the Company is required to maintain customer's KYC document as per the current CDD standards provided under this Policy. This is applicable even if there is no change in customer information but the documents available with the Operations department of the Company are not as per the CDD standards provided under this Policy. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Operations department of Company is required to undertake the KYC process equivalent to that applicable for onboarding a new customer.

b) The Operations department of the Company is to ensure verification of the Customer's PAN details, if available, from the database of the issuing authority at the time of periodic updation of KYC.

c) The Operations department of the Company is to provide an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation. Further, the Operations department of the Company is to ensure that it promptly updates the information / documents obtained from the customers at the time of updation / periodic updation of KYC in its records / database and provide an intimation, mentioning the date of updation of KYC details, to the customer.

5. The Operations department of the Company shall keep the Customers duly informed that, for the purpose of compliance with the applicable Rules, the Customers are required to submit to the Operations department of the Company updated documents in the event of any change or update to the documents submitted by the Customer at the time of establishment of the business relationship or account-based relationship, and thereafter, as and when required. The Operations department of the Company should ensure that its records are updated within a period of thirty (30) days from the date of receipt of such updated documents from the Customer.

6. Due Notices for Periodic Updation of KYC: The Company shall intimate customers in advance regarding periodic updation of KYC and issue reminders where the updation

remains pending, in the manner and at the intervals prescribed under applicable regulatory requirements. Such intimations and reminders shall be appropriately recorded in the Company's systems for audit trail purposes

The Company shall facilitate updation and periodic updation of KYC through appropriate arrangements consistent with its operating model and applicable regulatory requirements.

9.3 Maintenance of Records of Transactions

The Information Technology and Operations Department of the Company is required to maintain proper records of the transactions as required under the provisions of Act and Rules. Specifically, the Information Technology and Operations Department of the Company is to ensure that it:

1. maintains all necessary records of transactions between itself and the customer for at least five years from the date of transaction or any other higher periods specified under law;

2. preserves the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

3. swiftly makes available, the identification records and transaction data to the competent authorities upon request from such authority;

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

5. maintain all necessary information in respect of transactions prescribed under rule 3 of Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 so as to permit reconstruction of individual transaction, including the following:
   - the nature of the transactions;
   - the amount of the transaction and the currency in which it was denominated;
   - the date on which the transaction was conducted; and
   - the parties to the transaction.

6. maintain a system for proper holding and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

7. Where a customer is a non-profit organisation, the Company shall ensure that the customer's details are registered on the DARPAN Portal of NITI Aayog. If the customer is not already registered, the Company shall complete the registration process. The Company shall maintain records of such registration for five years after the business relationship has ended or the account has been closed, whichever is later.

10. Requirements and Obligations under International Agreements and Communications from International Agencies

Credit Risk department of the Company is to ensure compliance with the requirements and Obligations under International Agreements and Communications from International Agencies, provided under Chapter XI of the Master Direction, the said obligations include:

1. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967: Credit Risk department of the Company to ensure that in terms of section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals / entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

2. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005): Credit Risk department of the Company to ensure meticulous compliance with the 'Procedure for Implementation of section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005' laid down in terms of section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India, Annexed as Annex II of the Master Directions.

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

4. Jurisdictions that do not or insufficiently apply the FATF Recommendations:

    a. The Credit Risk department of the Company to keep a track of the FATF Statements circulated by the RBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF

Recommendations. The Credit Risk department of the Company is to apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

b. The Credit Risk department of the Company to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

c. The Credit Risk department of the Company to examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations, retain written findings together with all documents, and make them available to the RBI / other relevant authorities, on request.

The Company shall undertake screening of customers and transactions against applicable sanctions and designated-person lists at onboarding, on a periodic basis and at such frequency as may be prescribed. Any potential or confirmed match shall be promptly escalated and dealt with, including through reporting, prevention of transactions and freezing of funds or assets, wherever applicable, in accordance with the UAPA, WMD Act, applicable Government orders and regulatory directions.

11. Risk Management

1. The Compliance department of the Company to ensure that all departments work in co-ordination for implementation of the KYC policy. Heads of all the Departments will ensure that the respective responsibilities in relation to KYC policy are properly understood, given proper importance and appreciated and discharged with utmost care and attention by all the employees of the Company.

2. The Risk department of the Company will carry out periodic checks to determine as to whether all provisions of the KYC policy are being followed and adhered to by all the Departments concerned. The Audit Committee of the Board to ensure reviewing adherence to the KYC guidelines at periodic intervals. Compliance department of the Company to ensure submission of quarterly audit notes and compliance to the Audit Committee.

3. The Company's internal audit department is to periodically evaluate the level of adherence to the KYC procedures. Internal Audit department of the Company to also

provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements.

4. Compliance department of the Company to ensure that High risk accounts be subjected to intensified monitoring. The Credit Risk Department of the Company to also set key indicators for such high-risk accounts, based on factors mentioned under Section 5 of this policy document as well as the type of transactions involved (such as accounts having unusual transactions, inconsistent turnover, etc.) and other risk factors.

5. While ensuring compliance with the legal / regulatory requirements as above, the Company will also adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

12. General

12.1 Appointment of Designated Director

1. A 'Designated Director' means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the Rules and such direction is to be nominated by the Board. (b) The name, designation and address of the Designated Director be also communicated to the FIU-IND and to the Reserve Bank of India as required by law. (c) In no case, the Principal Officer be nominated as the 'Designated Director'.

12.2 Appointment of Principal Officer and reporting to Financial Intelligence Unit - India

1. To ensure effective implementation of this KYC Policy and a proper co-ordination and communication between the Company and RBI and other relevant enforcement authorities, the Company is required to designate a senior official Principal Officer (Managerial Level), who will operate from the corporate office of the Company.

2. The Compliance department of the Company to ensure that the name of the Principal Officer so designated, his designation and address including changes from time to time, is timely communicated to the Director, FIU-IND and to the Reserve Bank of India as required by law.

3. The Principal Officer to remain present at the Head / Corporate office of the Company.

4. Mr. Maria Francis, Head – Operations of the Company, has been appointed as the Principal Officer and the official responsible for ensuring fraud monitoring and reporting in accordance under the Master Direction and other applicable law.

5. The Principal Officer will report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the Rules, in the prescribed formats as designed and circulated by RBI at the following address:
   Director, FIU-IND,
   Financial Intelligence Unit, India,
   6th Floor, Hotel Samrat, Chanakyapuri,
   New Delhi - 110021.

6. Where the Principal Officer 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 Rules, such officer to furnish information in respect of such transactions to the Director, FIU-IND, within the prescribed time.

7. The Compliance department of the Company and the Principal Officer to ensure and take note of the reporting formats and comprehensive reporting format guide, prescribed / released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports.

8. The Principal Officer shall ensure that appropriate systems and arrangements are in place to identify, extract, compile and report transaction data from the Company's records and systems for the purpose of CTR, STR and other regulatory reporting requirements in the formats prescribed by FIU-IND from time to time.

9. The Compliance department of the Company, its directors, officers, and all employees to ensure that the fact of maintenance of records referred to in Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, and keep such information confidential. However, the confidentiality requirement are not intended to inhibit sharing of information or any analysis of transactions and activities, which appear unusual, with any of the other Kaleidofin Group entities, if the Compliance department of the Company has done any such analysis in this regard, under the Rules.

10. A copy of all information furnished is to be retained by the Principal Officer for the purposes of official record.

12.3 Hiring of Employees and Training

1. The Human Resources Department of the Company to have adequate screening mechanism as an integral part of personnel recruitment / hiring process and also should have an ongoing employee training programs so that members of the staff having business

and customer onboarding or risk management focused responsibilities are adequately trained in KYC/AML/CFT procedures. Training requirements should have different focuses for front line staff and officer/staff dealing with new customers and managing relationship with existing customers, so that all concerned fully understand the rationale behind the KYC policies and implement them consistently.

12.4 Sharing KYC Information with Central KYC Records Registry

1. The Company shall capture and upload customers' KYC records to CKYCR within ten days from commencement of an account-based relationship or within such other period as may be prescribed. The KYC information shall be captured and uploaded in the applicable CKYCR template and in accordance with the PML Rules, applicable regulatory requirements and the operational guidelines issued by CERSAI. KYC records of customers onboarded before the applicable CKYCR commencement dates shall be uploaded or updated at the time of periodic updation or earlier when updated KYC information is obtained from the customer, in accordance with applicable requirements.

2. The Company to procure the KYC information for sharing with the CKYCR in the manner mentioned in the Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as per the KYC templates prepared '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. The Company should ensure uploading the KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, in the LE template released by CERSAI.

2. Once KYC Identifier is generated by CKYCR, the Company should also ensure that the same is communicated to the respective customer.

3. Operations Department to ensure shall upload or update the KYC data of individual and legal entity customers in accordance with the timelines prescribed under applicable requirements.

4. Also, as and when Operations Department of Company obtains additional or updated information from any Customer, the same within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR.

5. Once CKYCR informs the Company regarding an update in the KYC record of an existing Customer, Operations Department of Company to retrieve the updated KYC records from CKYCR and update the KYC record maintained by the of Company.

6. Operations Department of Company is to ensure that during periodic updation, the

customers are migrated to the current CDD standard provided under this Policy.

7. For the purpose of establishing an account-based relationship, updation / periodic updation or for verification of identity of a customer, Operations Department of Company to seek and procure the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and not require a customer 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; or
   (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
   (iii) the validity period of downloaded documents has lapsed; or
   (iv) if the Operations Department of Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the Customer.

Where the Company downloads and relies upon current and compliant KYC records from CKYCR, it shall not be required to reverify the authenticity of the customer's identity or address. The Company shall, however, remain responsible for all other aspects of customer due diligence under applicable regulatory requirements.

12.5 Identification of Beneficial Owner:

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

   - Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such an entity.
   - In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place be obtained.
   - It is obligated to obtain the status of the trustees in following specific scenarios:
     i. When initiating an account-based relationship with the trust;

ii. When the trust, acting as a walk-in customer, conducts transactions involving a minimum of fifty thousand rupees;

iii. If the Company has reasonable grounds to suspect that the trust is intentionally structuring transactions to remain below the fifty thousand rupees threshold.

12.6 Group-Wide Policy

1. The structure, norms, standards and processes on including Anti Money Laundering and Countering Financing of Terrorism, as set out under this Policy, and processes/ policies for sharing information required for the purposes of CDD and money laundering and terror finance risk management as set out in this Policy, are to be implemented by companies/entities who are part of the Kaleidofin Group.

12.7 Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010:

1. The Compliance Department of Company to ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010, and rules made thereunder.

2. Further, the Compliance Department of Company to also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the RBI based on advice received from the Ministry of Home Affairs, Government of India.

12.8 Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards:

1. As required under FATCA and CRS, the Company to ensure adherence to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, it is required to take following steps for complying with the reporting requirements:

   (1) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution.

   (2) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

   Explanation: the Company to refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence

procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

(3) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

(4) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

(5) Constitute a 'High-Level Monitoring Committee' under the Designated Director or any other equivalent functionary to ensure compliance.

(6) Ensure compliance with updated instructions / rules / guidance notes / press releases issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the website http://www.incometaxindia.gov.in/Pages/default.aspx. REs may take note of the following:

(i) updated Guidance Note on FATCA and CRS; and
(ii) a press release on 'Closure of Financial Accounts' under Rule 114H (8).

12.9 Allocation of Authorities and Responsibility

1. For the purpose of effective implementation of this Policy, procedure and functions laid down herein, the allocation of authorities and responsibilities amongst the departments and functions of the Company are as hereunder:

Sr.	Name of Department / Function	Authorities	Responsibilities
1.	Board of Directors	Ultimate authority for KYC & AML governance	Approval of KYC & AML Policy and material amendments; overall oversight of AML/CFT framework; periodic review of policy effectiveness; ensuring adequate resources and systems for compliance
2.	Chief Risk Officer	Oversight authority delegated by the Board	Review of compliance with KYC & AML requirements; review of

			ML/TF Risk Assessment outcomes; monitoring regulatory observations and corrective actions; oversight of internal audit findings
3.	Designated Director	Statutory authority under PMLA	Ensuring overall compliance with obligations under PMLA, Rules and RBI Directions; acting as principal interface with RBI/FIU-IND on governance matters
4.	Principal Officer	Operational AML authority	Day-to-day AML/CFT compliance; filing STRs/CTRs and other regulatory reports with FIU-IND; coordination with regulators; escalation of suspicious activities; ensuring confidentiality of STRs
5.	Compliance	Policy interpretation and regulatory oversight authority	Interpretation of RBI/PMLA requirements; ensuring alignment of internal policies with regulatory changes; monitoring regulatory compliance; advisory support to Operations, Business and Risk; regulatory reporting coordination
6.	Operations	Execution authority for KYC processes	Customer onboarding and KYC verification; execution of approved customer identification processes; periodic KYC updation; CKYCR upload and retrieval; maintenance of KYC records; and ensuring

			completion of applicable CDD requirements prior to disbursement.
7.	Credit Risk	Risk assessment and monitoring authority	Customer risk categorisation; ML/TF Risk Assessment; enhanced due diligence for high-risk customers; transaction monitoring frameworks; defining red flags and escalation triggers
8.	Business & PeX	Facilitation authority (non-decision making)	Collection of customer information and documents through Business Partners, ensuring submission of complete KYC documents; adherence to KYC requirements as prescribed by Compliance and Operations
9.	Information Technology	Systems and infrastructure authority	Maintenance of KYC, AML and transaction monitoring systems; system controls for audit trails; data integrity and security; integration with CKYCR, DigiLocker, sanctions screening tools; system support for approved KYC processes
10.	Internal Audit	Independent assurance authority	Periodic audit of KYC & AML processes; testing of compliance with policy and RBI directions; verification of effectiveness of controls; reporting gaps and recommendations to Audit Committee

11.	Human Resources	Training and people-governance authority	Employee screening at onboarding; periodic KYC/AML training; ensuring staff awareness of AML/CFT obligations; maintaining training records
12.	Customer Engagement	Customer interface authority	Handling customer queries related to KYC; support for KYC updation; guiding customers on documentation requirements; escalation of suspicious patterns noticed during interactions

12.10 Operation of accounts and Money Mules

1. The Credit Risk Department of Company to ensure that the instructions on opening of accounts and monitoring of transactions be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to accounts by recruiting third parties which act as "money mules."

2. The Credit Risk Department of Company to ensure and undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND.

3. The Company to allot Unique Customer Identification Code (UCIC) while entering into new relationships with individual customers as also the existing individual customers.

12.11 New Products Launch

1. The Company to 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 existing products. Further, the Credit Risk Department of Company to ensure:

   (i) to undertake the ML / TF risk assessments prior to the launch or use of such

products, practices, services, technologies; and

(ii) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

12.12 Wire transfer / Fund Transfers Related to Lending Operations

KCPL does not undertake remittance, money transfer, payment intermediary, correspondent banking, or cross-border transfer activities. Loan disbursements and collections are routed through regulated banking channels. Wherever KCPL originates fund transfers in connection with lending operations, it shall ensure that customer identification records are maintained and that transfers are made only through verified customer bank accounts. Any unusual fund movement patterns, third-party repayments, or transactions inconsistent with the customer's profile shall be subject to enhanced scrutiny and reporting requirements under applicable AML regulations.

12.13 Third Party Products

1. In cases where the Company acts or proposing to act as agent while selling third party products as per regulations in force from time to time, in such case, Operations Department of Company to ensure compliance with the following aspects for the purpose of the Master Direction:

   (1) the identity and address of the walk-in customer be verified for transactions above ₹50,000 as required under paragraph 7(1)(e) of this Policy.
   (2) transaction details of sale of third-party products and related records be maintained as prescribed in paragraph 8.3 of this Policy.
   (3) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers be available.
   (4) transactions involving ₹50,000 and above be undertaken only by:

      (i) debit to customers' account or against cheques; and
      (ii) obtaining and verifying the PAN given by the account-based as well as walk-in customers.

   (5) Instruction at (4) above to also apply to sale of the Company's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for ₹50,000 and above.

ANNEXURE I
Digital KYC Process

(The Company is currently not undertaking Digital KYC process. As and when this process is initiated in the future, it shall ensure compliance with the applicable requirements)

Digital KYC Process:

(1) The Company may develop an application for digital KYC process and make it available at customer touch points for undertaking KYC of its customers and is required to undertake the KYC process only through this authenticated application.

(2) The Company shall control the access to the Application and ensure that unauthorised persons do not use it. Authorised officials are to access the Application only through a login-id and password or a Live OTP or Time OTP controlled mechanism that the Company provides.

(3) The customer, for the purpose of KYC, is required to visit the location of the authorised official of the the Company or vice-versa. The original OVD is required to be in possession of the customer.

(4) The Company is required to ensure that the authorised officer takes a Live photograph of the customer and embeds the same photograph in the Customer Application Form (CAF). Further, the Company's system Application is required to put a watermark in readable form, containing the CAF number, GPS coordinates, authorised official's name, unique employee code (which the the Company assigns) and date (DD:MM:YYYY) and time stamp (HH:MM:SS), on the captured live photograph of the customer.

(5) The Company's Application is required to have the feature that it captures only a live photograph of the customer and does not capture any printed or video graphed photograph. The background behind the customer while capturing live photograph is required to be of white colour and no other person is required to come into the frame while capturing the live photograph of the customer.

(6) Similarly, the authorised officer is required to capture the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), vertically from above and is required to apply a water-marking in readable form as mentioned above. The authorised officer is required to ensure there is no skew or tilt in the mobile device while capturing the live photograph of the original documents.

(7) The authorised officer is required to capture the live photograph of the customer and his original documents in proper light so that they are clearly readable and identifiable.

(8) Thereafter, the authorised officer is required to fill all the entries in the CAF as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details may be auto-populated by scanning the QR code instead of manual filing the details.

(9) 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 required to be sent to customer's own mobile number. In any case, the authorized person is required not to use the his/her mobile number for the customer signature. The Company is to ensure that the mobile number used in customer signature is not the mobile number of the authorised officer.

(10) The authorised officer is to provide a declaration about the capturing of the live photograph of the customer and original document. For this purpose, the Company is required to verify the authorised officer with One Time Password (OTP). Upon successful OTP validation, the Company is to treat it as the authorised officer's signature on the declaration. The live photograph of the authorised officer is required to be captured in this authorised officer's declaration.

(11) Subsequent to all these activities, the Application is required to give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the transaction-id / reference-id number of the process. The authorised officer is required to intimate the details regarding transaction-id / reference-id number to the customer for future reference.

(12) The authorised officer of the Company to check and verify that:

(i) information available in the picture of the document matches with the information entered by authorised officer in CAF.

(ii) live photograph of the customer matches with the photo available in the document.; and

(iii) the authorised officer has properly filled all of the necessary details in CAF, including mandatory field.

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

Non-Face-To-Face OTP based e-KYC

(1) For Non-Face-To-Face OTP based e-KYC the authorised officer of the Company is first required to procure specific consent for the authentication through OTP.

(2) As a risk-mitigating measure for such accounts, the Company is to ensure that it sends transaction alerts, OTP, etc., only to the mobile number of the customer registered with Aadhaar. The Company may change the mobile number for such customer and account who requests for or Non-Face-To-Face OTP based e-KYC after complying the following procedure.

a. When any customer request for change of his registered mobile, the Company shall update the same basis the writen request from the customer.

(3) The aggregate balance of all the accounts of the customer to remain under and not exceed Rupees One Lakh. In case the balance exceeds the threshold, operations of such account ceased, until it completes the CDD as mentioned at (6) below.

(4) The aggregate of all credits in a financial year, in all the accounts taken together, to remain under and not exceed the threshold of Rupees Two Lakh.

(5) As regards borrowal accounts, the Company is to ensure that it sanction only term loans of the customers opting for Non-Face-To-Face OTP based e-KYC and the aggregate amount of such term loans sanctioned is to remain below not exceed ₹60,000 in a year.

(6) The Company is to not allow accounts opened using OTP based e-KYC to operate for more than one year unless it carries out identification as Para no. 7 (*Customer Identification Procedure*) and Para no. 8 (*Customer Due Diligence*) of the Policy or the V-CIP procedure as per **Annexure II** of the Policy . If the Company uses Aadhaar details it is to follow the process in its entirety, including fresh Aadhaar OTP authentication.

(7) If the Company does not complete the CDD procedure as mentioned above within a year, in respect of borrowal accounts, there shall be no further debits from such account.

(8) The Company is to obtain declaration 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 RE. Further, while uploading KYC information to CKYCR, the Company is to ensure that it clearly indicate that such accounts are opened using OTP based e-KYC and other REs are not to open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face- to-face mode.

(9) The Company to have have strict monitoring procedures including systems to generate alerts in case of any non-compliance / violation, to ensure compliance with the above-mentioned conditions.

ANNEXURE II
V-CIP Process

(The Company is currently not undertaking V-CIP process. As and when this process is initiated in the future, it shall ensure compliance with the applicable requirements)

The Company may undertake V-CIP, for the applicable cases as follows:

(1) CDD in case of new customer onboarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

(2) *Provided that* in case of CDD of a proprietorship firm, the Company to also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in paragraph 8(2)(b) and paragraph 8(2)(c) of this Policy, apart from undertaking CDD of the proprietor.

(3) Conversion of existing accounts opened in non-face-to-face mode using Aadhaar OTP based e-KYC authentication as per procedure provided under Annexure II of this Policy.

(4) Updation / Periodic updation of KYC for eligible customers.

The Company is to ensure that the standards are maintained for V-CIP facility:

(1) V-CIP Infrastructure

(i) The Company to ensure compliance with the RBI guidelines on minimum baseline cyber security and resilience framework for NBFC, as updated from time to time as well as other general guidelines on IT risks.

(ii) The Company to house the technology infrastructure at its office premises and the V-CIP connection and interaction in that regard be necessarily originated from its own secured network domain. Any technology related outsourcing for the process in that respect to be ensured to remain in compliance with relevant RBI guidelines.

(iii) In case, the Company uses a cloud deployment model, it in such cases the Company is to ensure that that ownership of data in such model rests with the only with the Company and all the data including video recording is transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and the Company is to ensure that the cloud service provider or third-party technology provider assisting the V-CIP do not retain any data.

(iv) The Company to 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 Company is to ensure recording the customer consent in an auditable and

alteration-proof manner.

(v) The Company to ensure the V-CIP infrastructure / application is capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

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

(vii) The Company to ensure that the application have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy. The responsibility of customer identification rests with the Company.

Explanation: Making specific facial gestures, like blinking of eyes, smiling, frowning, etc. is not mandatory for liveness check. The Company may take due cognizance of special needs, if any, of the customer during liveness check.

(viii) The Company may also use appropriate artificial intelligence (AI) technology to ensure that the V-CIP is robust.

(ix) The Company to regularly update the technology infrastructure including application software as well as workflows based on experience of detected / attempted / 'near-miss' cases of forged identity. The Company is to ensure reporting any detected case of forged identity through V-CIP as a cyber event under extant regulatory guidelines.

(x) The Company to ensure that the V-CIP infrastructure is subjected to necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. The Company to ensure mitigation of any critical gap reported under this process before rolling out its implementation. The empanelled auditors of Indian Computer Emergency Response Team (CERT-In) be assigned the work to conduct such tests. Further the said tests shall be carried out periodically in conformance to internal / regulatory guidelines.

(xi) The Company to subject the V-CIP application software and relevant APIs / webservices to appropriate testing of functional, performance, and maintenance strength before being used in live environment. The Company to roll out the application only after closure of any critical gap found during such tests. The Company shall carry out such tests periodically in conformity with internal / regulatory guidelines.

(2) V-CIP Procedure

(i) The Company is required to formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The Company to ensure that V-CIP process is operated only by officials of the Company specially trained for this purpose. The official of said the Company be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The Company to ensure that liveness check process does not result in exclusion of person with special needs.

(ii) The Company to ensure that the disruption of any sort including pausing of video, reconnecting calls, etc., may not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then the Company is not required to initiate a fresh session. However, in case of call drop / disconnection, fresh session is to be initiated.

(iii) The Company is to ensure variable sequence and / or type of questions, including those indicating the liveness of the interaction, during video interactions to establish that the interactions are real-time and not pre-recorded.

(iv) The Company ensure that the account opening process is rejected if any prompting at observed from the customer end.

(v) The Company to ensure checking in the fact if the V-CIP customer is an existing or new customer, or if the case relates to one rejected earlier or if the name appears in some negative list, at an appropriate stage of workflow.

(vi) The authorised official of the Company performing the V-CIP to ensure recording audio and video as well as capture a photograph of the customer present for identification and obtain the identification information using any one of the following:

(a) OTP based Aadhaar e-KYC authentication.

(b) Offline Verification of Aadhaar for identification.

(c) KYC records downloaded from CKYCR, in accordance with paragraph 12.4, using the KYC identifier provided by the customer.

(d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.

(vii) The Company to redact or blackout the Aadhaar number in terms of paragraph 8(1) of this Policy.

(viii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the Company is to ensure that the XML file or QR code generation date is not older

than three working days from the date of carrying out V-CIP.

(ix) Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the Company is also required to ensure that it undertakes video process of the V-CIP 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, the Company to ensure that no incremental risk is added due to this.

(x) If the address of the customer is different from that indicated in the OVD, the Company to capture suitable records of the current address, as per the existing requirement. The Company is to also ensure that it confirms the economic and financial profile / information submitted by the customer from the customer undertaking the V-CIP in a suitable manner.

(xi) The Company to ensure capturing a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The Company is to verify the PAN details from the database of the issuing authority ,including through DigiLocker.

(xii) The use of printed copy of equivalent e-document, including an e-PAN is not valid for the V-CIP.

(xiii) The authorised official of the Company is to ensure that photograph of the customer in the Aadhaar / OVD and PAN / e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar / OVD and PAN / e-PAN is matched with the details provided by the customer.

(xiv) The Company is to make all accounts opened through V-CIP operational only after subjecting them to concurrent audit to ensure the integrity of process and its acceptability of its outcome.

(xv) The Company to also ensure compliance with all requirements provided under law including the Information Technology Act, in addition to the requirements provided under the Master Directions.

(3) V-CIP Records and Data Management

(i) The Company is to store the entire data and recordings of V-CIP in a system / system located in India. The Company is to ensure that the video recordings are 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 under the Master Directions, also apply to V-CIP.

(ii) The Company is to ensure preservation of the activity log along with the credentials of the official performing the V-CIP.

***

MODIFICATION TRACKER

Version	Date	Reviewed by	Approved by	Remarks
2.0	27-Jul-2022	Puneet Gupta & Sucharita Mukherjee	Board	-
2.1	21-Jul-2023	Puneet Gupta	Board	Annual review
2.2	01-Mar-2024	Puneet Gupta	Board	Annual review
2.3	-	Puneet Gupta	Board	Annual review
3.0	10-Oct-2024	Puneet Gupta	Board	Updations
3.1	25-Sept-2026	Samvad, Francis, Deepak, Sindhuja	Board	Annual review

