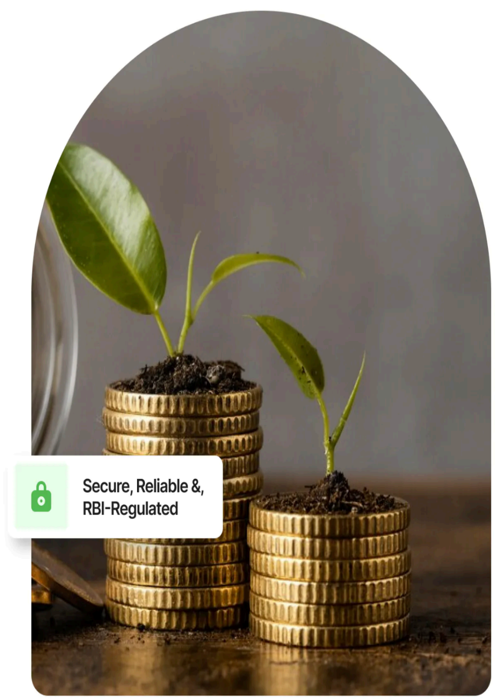
AMBIUM FINSERVE LIMITED
(FORMERLY AMBIUM FINSERVE PRIVATE LIMITED)

Empowering Businesses with Personalised Financial Solutions

Unlock opportunities with our personalised B2B loans, crafted to drive your business forward.



KNOW YOUR CUSTOMER (KYC), ANTI MONEY LAUNDERING (AML), COMBATING FINANCING OF TERRORISM (CFT) AND CUSTOMER ACCEPTANCE POLICY (CAP)

Document Versioning

Name of the document	**KNOW YOUR CUSTOMER (KYC), ANTI MONEY LAUNDERING (AML), COMBATING FINANCING OF TERRORISM (CFT) AND CUSTOMER ACCEPTANCE POLICY (CAP**
Issuing Authority	Board of Directors
Effective date of the Policy	3rd January 2024
Policy Owner	Chief Investment Officer
Last reviewed on	18th June 2026
Next review date	15 June 2027, if required

Version History

Version	Revision Summary	Approving Authority	Effective Date
0	Original	Board of Directors	1 June 2017
1	Version 1	Board of Directors	27 September 2023
2	Version 2	Board of Directors	3rd January 2024
3	Version 3	Board of Directors	29th May 2025
4	Version 4	Board of Directors	18th June 2026

Table of Content

I. INTRODUCTION AND BACKGROUND

Ambium Finserve Limited (Formerly known as Ambium Finserve Private Limited) ("the Company" or "Ambium") is a Non-Systemically Important Non deposit taking Non-Banking Financial Company (NBFC-ND-NSI) duly registered with the Reserve Bank of India (RBI). Under the Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025, the Company is categorized as a Base Layer NBFC based on its asset size.

The Company is engaged in the business of providing secured as well as unsecured business loans to the under-served individuals, households, and businesses and offer wholesale lending to other NBFCs and Financial Institutions and body Corporates (having an AUM of up to INR 5000 crores or such other cap as may be decided by the Board) to provide access to credit to under-served segment.

In terms of the provisions of Prevention of Money Laundering (PML) Act, 2002 ("PML Act / PMLA/Act") and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Rules/ Rules"), as amended from time to time by the Government of India and as notified by the Government of India, Non-Banking Financial Companies (NBFCs) being Regulated Entities (REs) are required to follow certain customer identification procedures and conduct customer due diligence while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions and take steps to ensure implementing the provisions of the aforementioned Act, Rules and Ordinance, including operational instructions issued in pursuance of such amendment(s).

Accordingly, the Company has adopted this KYC/AML/CFT and CAP Policy ('the Policy') in line with the requirements of the RBI's Master Direction - Know Your Customer (KYC) Direction, 2016, as updated from time to time. This policy has been duly approved by the Board of Directors of the Company.

II. OBJECTIVE AND SCOPE

The objective of this Policy is to:

- prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities;
- enable the Company to know/ understand its customer and their financial dealings better, which in

turn helps to manage its risks prudently;

- establish a proper Customer Due Diligence ("CDD") process before on-boarding Customers including the process of customer acceptance, customer identification and monitoring of transactions; and
- comply with all the legal and regulatory obligations in respect of KYC, AML and CFT measures.

The provisions of this Policy shall be applicable to all the customers, employees, products, services and all the other relevant stakeholders of the Company and the procedures mentioned herein shall be carried out for all business verticals.

III. KEY DEFINITIONS

The terms herein shall bear the meanings assigned to them below:

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

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

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

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

iv. "Beneficial Owner" (BO) -

a. Where the **customer is a company**, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
Explanation- For the purpose of this sub-clause

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 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. 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.

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

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

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

- authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident
- customer resides.

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

vii. "Customer" A customer for the purpose of KYC Policy is defined as:

- A person or entity that maintains an account and/or has a business relationship with the Company; or
- One on whose behalf the account is maintained (i.e., the beneficial owner); or
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.
Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

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

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

x. "Group" – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

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

xii. "Officially Valid Document" (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,
a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at (b) above

d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name. “Offline verification” shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xiii. “Person” has the same meaning assigned in the Act and includes:

a) an individual,
b) a Hindu undivided family,
c) a company,
d) a firm,
e) an association of persons or a body of individuals, whether incorporated or not, f) every artificial juridical person, not falling within any one of the above persons (a to e), and g) any agency, office or branch owned or controlled by any of the above persons (a to f).

xiv. “Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions by India or a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials or as defined under the RBI Master Direction - KYC Directions, 2016, Prevention of Money-laundering (Maintenance of Records) Rules, 2005 and such other applicable rules and regulations.

xv. “Principal Officer” means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

xvi. “Suspicious transaction” means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

b) appears to be made in circumstances of unusual or unjustified complexity;
or c) appears to not have economic rationale or *bona-fide* purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

xvii. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery, or the arrangement thereof and includes:
a) opening of an account;
b) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
c) the use of a safety deposit box or any other form of safe deposit;
d) entering into any fiduciary relationship;
e) any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f) establishing or creating a legal person or legal arrangement.

(b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "Customer" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

ii. "Walk-in Customer" means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.

iii. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

iv. "Customer identification" means undertaking the process of CDD.

v. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

vi. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

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

viii. "Periodic Updation" means steps taken to ensure that documents, data, or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

ix. "Regulated Entities" (REs) means –

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)

d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

e. All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

IV. KEY ELEMENTS OF THE POLICY

1. Customer Acceptance Policy
2. Customer Identification Procedures
3. Customer Due Diligence
4. Risk Management
5. Monitoring of Transactions

1. Customer Acceptance Policy ("CAP")

The Customer Acceptance Policy lays down explicit criteria for acceptance of customers. The Policy ensures that the following procedures shall be followed in relation to customers who approach for availing financial facilities with the Company:

a. No account shall be opened or transaction shall be executed in anonymous or fictitious/benami names or on behalf of other persons whose identity has not been disclosed or cannot be verified.

b. Parameters of risk perception in terms of monitoring Suspicious Transactions) shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc.

c. Customer shall be categorized as low, medium, and high risk.

d. No transaction is undertaken where the company is unable to apply appropriate CDD as set out in this policy, either due to non-cooperation of the customer or non-reliability of the data/information furnished to the company.

e. The Company shall collect documents and other information from the customer depending on perceived risk and considering the requirements of PMLA Act, 2002, Rules and guidelines issued by RBI from time to time. Additional information shall be obtained with the explicit consent of the customer.

f. A Unique Customer Identification Code (UCIC) shall be allotted to new and all the existing customers. Appropriate CDD procedure shall be applied at the UCIC level. Thus, if an existing KYC compliant customer of Ambium desires to open another account with Ambium, there shall be no need for a fresh CDD exercise.

g. CDD Procedure shall be complied for all the joint account holders account, if applicable.

h. Circumstances in which a customer is permitted to act on behalf of another person/entity, must be clearly spelt out.

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

j. Where PAN and GST details have been made available the same shall be verified from the search/verification facility of the issuing authority.

k. The Company shall ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by the RBI or if the person or entity is found to be even remotely associated with any individual terrorist or prohibited/ unlawful organisations as notified by RBI, Government of India and other relevant national or international organisations. The Company shall at all times comply with the requirements of the provisions of Chapter IX of the Master Directions on KYC issued by the RBI in this regard.

l. Where there is a suspicion of money laundering or terrorist financing and it is believed that performing CDD will tip-off the customer, CDD shall not be pursued and instead an STR shall be filed with FIU-IND for the same.

m. Records or the information of the customers due diligence carried out through the records of CKYCR shall be obtained by the Company within 2 days from the Central KYC Records Registry.

n. The Company shall have an option of establishing relationship with Politically Exposed Persons (“PEPs”) subject to:

i. sufficient information including information about the sources of funds accounts of family members and close relatives shall be gathered on the PEP;

ii. the identity of the person shall have been verified before accepting the PEP as a customer; iii. the decision to open an account for a PEP is taken at a senior level in accordance with this Customer Acceptance Policy;

iv. all such accounts shall be subjected 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, senior management’s approval shall be obtained to continue the business relationship; and

vi. the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

The aforesaid measures shall be applicable in cases where PEP is the beneficial owner of a Legal Entity.

The Company shall not outsource the decision-making function of determining compliance with KYC norms.

2. Customer Identification Procedures ("CIP")

The Company shall identify the customers and verify their identity by using reliable, independent source documents, data, or information in case of individual as well as corporate. It shall ensure adherence of Customer Identification Procedure as prescribed by the RBI from time to time.

The Company shall ensure that Customer identification process is undertaken, whenever;

a. an account-based relationship is being established;
b. there is doubt about the authenticity or adequacy of customer identification data already obtained;
c. Ambium wants to satisfy itself about current address by obtaining required proof. For customers that are natural persons, the Company shall obtain enough identification data to verify the identity of the customer, his address/location, and his recent photograph. Customer Identification requirements in respect of a few typical cases, are given in ***Annexure 1*** for the guidance of the Company.

3. CUSTOMER DUE DILIGENCE ("CDD") PROCEDURE

a. In case of Legal Persons or Entities:

For customers that are legal persons or entities, the Company shall:

- verify the legal status of the legal person/ entity through charter documents and tax registration etc.
- verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person through authentic documents and
- understand the ownership and control structure of the customer and determine who are the natural persons ultimately controlling the legal person.

The list of documents to be collected and verified depending upon their nature is specified in below table:

Types of entity	Type of document to be collected and verified

Sole Proprietary firms	In addition to performing CDD applicable in case of an Individual (for the proprietor) any two of the following documents must be obtained as a 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/license issued by the municipal authorities under Shop and Establishment Act iii. Sales and income tax returns iv. CST/VAT/ GST certificate (provisional/final) v. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities vi. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License/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. iii. Utility bills such as electricity, water, landline telephone bills, etc. *The Company may, at the time of undertaking Contact Point Verification, ask for additional documents, if required, for establishing the existence of the firm and confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.*
Corporate (Public Limited/ Private Limited Company)	In addition to performing the CDD applicable in case of Individuals (for beneficial owners, authorised signatories, POA holders. etc.) certified copies of each of the following documents or the equivalent e-documents of the Company shall be obtained: i. Certificate of Incorporation ii. Updated 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 apply, open, and operate the loan on its behalf

	v. Documents specified above for individuals relating to beneficial owner, the 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 senior management position; and vii. the registered office and the principal place of its business if it is different.

Partnership Firms	In addition to performing the CDD applicable in case of Individuals (for partners, beneficial owners, authorized signatories, POA holders. etc.) certified copies of each of the following documents or the equivalent e documents of the Firm shall be obtained: i. Registration Certificate ii. Partnership Deed iii. PAN of the Partnership Firm iv. Documents, as specified in Section 16, relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf v. The names of all the partners; and vi. Address of the registered office, and the principal place of business, if it is different

Trust	In addition to performing the CDD applicable in case of Individuals (for beneficial owners, authorized signatories, POA holders. etc.) certified copies of each of the following documents or the equivalent e-documents of the Trust shall be obtained: i. Registration certificate ii. Trust deed iii. Permanent Account Number or Form No.60 of the trust iv. Documents, as specified in Section 16, relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf v. the names of the beneficiaries, trustees, settlor, and authors of the trust vi. the address of the registered office of the trust; and vii. list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorized to transact on behalf of then trust.
Unincorporated association or a body of individuals & Unregistered trust/ partnership firms/ societies	In addition to performing the CDD applicable in case of Individuals (for beneficial owners, authorized signatories, POA holders. etc.) certified copies of each of the following documents or the equivalent e-documents of the unincorporated association or a body of Individuals shall be obtained: i. Resolution of the managing body of such association or body of individuals ii. Permanent Account Number 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, as specified in Section 16, relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf; and v. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

b. In case of Individuals:

For undertaking CDD, the Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with individual who is a beneficial owner, authorized signatory or power of attorney holder related to any legal entity:

i. The proof of possession of Aadhaar number where offline verification can be carried out; or
ii. The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
iii. the KYC Identifier with an explicit consent to download records from CKYCR; and
iv. the Permanent Account Number or the equivalent e-document thereof or where PAN is not available, Form No. 60 as defined in Income-tax Rules, 1962 (Mandatory); and
v. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the RE:

Note:

- A certified copy of Officially Valid Documents (OVD) as mentioned above in this policy, containing details of proof of their identity and address may also be accepted.
- Wherever Aadhaar details are collected, it shall be ensured that customers have redacted or blacked out their Aadhaar numbers through appropriate means.

3.1. Sharing of KYC information with CKYCR

i. Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

a. there is a change in the information of the customer as existing in the records of CKYCR; b. the current address of the customer is required to be verified;
c. the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client. d. the validity period of documents downloaded from CKYCR has lapsed.

ii. It must be ensured that, in terms of provision of Rule 9(1A) of the PML Rules, the Company shall capture customer’s KYC records and upload onto CKYCR within such timeline as maybe applicable.

iii. Further, in case of customers whose KYC records are being uploaded for the first time on the CKYCR system, it must be ensured that once KYC Identifier is generated by CKYCR, the same shall be communicated to the individual/LE as the case may be.

4. RISK MANAGEMENT

4.1. Risk Categorization

i. The overall responsibility, implementation and adherence of this Policy shall lie with the Board. The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures.
ii. The compliance function shall provide an independent evaluation of the Company own policies and procedures, including legal and regulatory requirements. The Company shall ensure that the audit machinery of the Company is staffed adequately with individuals who are well versed in such policies
and procedures.

iii. Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures at the Company and comment on the lapses observed in this regard. The compliance in this regard shall be put up before of the Board at such intervals as required. Risk Categorization
iv. All the customers under different product categories shall be categorized into low, medium, and high risk based on their profile.
v. The risk categorization can be done based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc. An indicative categorization for the guidance of businesses is provided in ***Annexure 2***.
vi. The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

4.2. Money Laundering and Terrorist Financing Risk Assessment

i. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions, or delivery channels, etc.
ii. While assessing the above risks, the Company 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, the Company shall take cognizance of the overall sector specific vulnerabilities, if any, that the regulator/supervisor may share with Company from time to time.
iii. The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be performed at least annually.
iv. The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and the same should be made available to competent

authorities and self-regulating bodies.

4.3 Periodic Updation of KYC

The Company shall adopt a risk-based approach for periodic updation of KYC. The periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account/ last KYC updation.

a. In case of Individuals:

i. No change in KYC information:

In case there is no change in the KYC information already submitted by the customer, a self declaration in this regard shall be obtained through customer's email-id or customer's mobile number registered with the Company, letter, etc.

ii. In case of change only in address

A self-declaration of the new address shall be obtained from the customer through customer's email-id or customer's mobile number registered with the Company, letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. Further, the Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

b. In case of Legal Persons or Entities ("LE"):

i. No change in KYC information: In case of no change in the KYC information of the LE customer, a self declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, letter from an official authorized by the LE in this regard, board resolution, etc. Further, details with regards to the status of the Beneficial Ownership (BO) information available with the Company shall be confirmed with the LE and updated, if required.

ii. Change in KYC information:

In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer.

iii. Further, the Company shall advise its customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary, customers shall submit to the Company the update of such documents within 30 days of the update to the documents for the purpose of updating the records at Company's end.

iv. **Additional Measures:** In addition to the above, Ambium shall ensure that -

a) Copies of the documents produced as Proof of Identity and Address shall be obtained and retained with the Company, wherein a responsible Company Official has to attest such copies certifying that the originals thereof have been verified.
b) The information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes.
c) It must be ensured that the KYC documents of the customer available with the Company shall always be as per the current CDD standards. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on boarding a new customer.
d) PAN details of all the customers must be verified from the database of the issuing authority.
e) Acknowledgement shall be provided to the customer specifying the date of receipt of the documents, including self-declaration.
f) Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
g) **In case of Existing Customers:** It must be ensured that PAN or Form 60 or equivalent e- document must be obtained from all the customers of the Company, failing which operations shall temporarily be ceased in such account until PAN or such documents have been submitted by the customers. Before ceasing the accounts, the customer must be intimated and an opportunity of being heard must be given. In case whereas customer denies submission of PAN card the Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Note: For the purpose of this Section, "temporary ceasing of operations" shall mean *"in case of loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed."*

4.4 Measures to be adopted while dealing with jurisdictions that do not or insufficiently apply the FATF Recommendations

i. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account. Special attention shall be given 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.

Explanation: The processes referred to in (i) & (ii) above do not preclude the Company from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

ii. 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 shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

5. MONITORING OF TRANSACTIONS

The Company shall undertake an on-going due diligence/ monitoring of transactions of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business, and risk profile; and the source of funds shall be undertaken on an on-going basis.

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

i. Any unusual pattern in the operations of the accounts which seems inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose, shall be closely monitored.

ii. Transactions which exceed the thresholds prescribed for specific categories of accounts.

The extent of monitoring shall be aligned with the risk category of the customer. Further, High risk accounts shall be subjected to more intensified monitoring.

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 shall be put in place.

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

V. RECORD MANAGEMENT

The Company shall introduce a system of proper maintenance and preservation of account information prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML

Rules, 2005). The following steps shall be taken regarding maintenance, preservation, and reporting of customer account information, with reference to provisions of PML Act and Rules. The Company shall:

i. maintain all necessary records of transactions between the Company and the customer for at least five years from the date of transaction;
ii. preserve 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;
iii. make available swiftly, the identification records and transaction data to the competent authorities upon request;
iv. maintain all necessary information in respect of transactions prescribed under PML Rule 3*(to the extent applicable and relevant) so as to permit reconstruction of individual transaction, including the following:
   a) the nature of the transactions;
   b) the amount of the transaction and the currency in which it was denominated;
   c) the date on which the transaction was conducted; and
   d) the parties to the transaction. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

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

*The company shall maintain all necessary information in respect of the following types of transactions as per the requirements of PMLA Rule 3:

i. all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
ii. all series of cash transactions integrally connected to each other which have been individually valued below Rupees Ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Ten lakh rupees or its equivalent in foreign currency;
iii. all transactions involving receipts by non-profit organisations of value more than Rupees Ten lakh, or its equivalent in foreign currency
iv. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
v. all suspicious transactions whether or not made in cash and by way of –

   a. deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of—

(i) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or

(ii) travelers' cheques, or

(iii) transfer from one account within the same banking company, financial institution, and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or

(iv) any other mode in whatsoever name it is referred to;

b. credits or debits into or from any non-monetary accounts such as demat account, security account in any currency maintained by the banking company, financial institution, and intermediary, as the case may be;

c. money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:—

(i) payment orders, or

(ii) cashiers' cheques, or

(iii) demand drafts, or

(iv) telegraphic or wire transfers or electronic remittances or transfers, or

(v) internet transfers, or

(vi) Automated Clearing House remittances, or

(vii)lock box driven transfers or remittances, or

(viii) remittances for credit or loading to electronic cards, or

(ix) any other mode of money transfer by whatsoever name it is called;

d. loans and advances including credit or loan substitutes, investments, and contingent liability by way of—

(i) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, interbank participation or any other investments in securities or the like in whatever form and name it is referred to, or

(ii) purchase and negotiation of bills, cheques, and other instruments, or

(iii) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or

(iv) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support

e. collection services in any currency by way of collection of bills, cheques, instruments, or any other mode of collection in whatsoever name it is referred to.

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

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

VI. KEY APPOINTMENTS

a. ***Principal Officer:*** As per the requirement of the PML Rules, Mr. Animesh Gupta has been appointed as the Principal Officer of the Company. Further details of the Principal Officer shall be intimated to FIU-IND and the Reserve Bank of India. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and reporting any transactions/information as covered under the PML Act read with its Rules.

b. ***Designated Director:*** As per the requirement of the PML Rules, Mr. Anshul Gupta has been appointed as the Designated Director of the Company. Further details of the Designated Director shall be intimated to FIU-IND and the Reserve Bank of India. Designated Director shall be responsible to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

c. ***Senior Management:*** To be in compliance with obligations provided under the PML Act, the Senior Management shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. In this regard, the senior management of the Company ("**Senior Management**") shall comprise of such people as may be decided by the Company from time to time.

VII. REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA ("FIU-IND")

i. In terms of the Rules, the Company is required to report information relating to cash (if applicable) and suspicious transactions electronically to FIU India. The Company shall comply with such reporting requirement by utilizing the formats stipulated in the Master Directions and as prescribed by FIU IND.

ii. The Cash Transaction Report (CTR) (for cash transactions and integrally connected cash transactions , transactions involving receipts by non-profit organizations, cash transactions where forged or counterfeit currency notes or bank notes have been used and cross border wire transfers, every month, as referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 of the PML Rules) for each month shall be submitted to FIU-IND by 15th day of the succeeding month.

iii. In case of all suspicious transactions referred to in clause (D) of sub-rule (1) of rule 3 of the PML Rules) for each month shall be submitted to FIU-IND within 7 working days on being satisfied that the transaction is suspicious.

iv. The Suspicious Transaction Report (STR) shall be submitted within 7 working days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

In this regard, the Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

v. The Company shall keep in mind that any delay in furnishing of information would result into a violation of the requirement stipulated in the Rules.

vi. The Principal Officer will be responsible for timely submission of STR to FIU-IND. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported. Details of accounts resembling any of the individuals / entities 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) shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

vii. The Company will not put any restrictions on operations in the accounts where an STR has been made. The Company shall keep the fact of furnishing of STR strictly confidential and its directors, officers, and employees (permanent and temporary) will be prohibited from disclosing ('tipping off') the fact that an STR or related information is being reported or provided to the FIU-IND.

This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be the duty of all employees involved to ensure that there is no tipping off to the customer at any level.

VIII. OTHER INSTRUCTIONS

i. **Introduction of New Technologies:** The Company will pay special attention to any money laundering threats that may arise from new or developing technologies.

ii. **Selling of Third-Party Products:** While acting as an agent while selling third party products as per regulations in force from time to time shall comply with the following aspects:

a. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand;

b. transaction details of sale of third-party products and related records shall be maintained;

c. 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 shall be available.

d. Transaction involving rupees fifty thousand and above shall be undertaken only

by: ○ debit to customers' account or against cheques; and
○ obtaining and verifying the PAN given by the account based as well as walk-in customers.

e. Instruction at 'd' above shall also apply to sale of REs' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

iii. Hiring of Employees and Employee training:

a. Hiring of Employees

The company shall ensure adequate due diligence from an AML perspective before employing any personnel including temporary/ outsourced manpower.

The role of employees in implementing AML framework being critical, employees would be expected to carry out the stipulated procedure efficiently. Any inefficient or suspicious behavior of employees shall be dealt with suitably. It shall be ensured that there is no tipping off to the customer at any level.

b. Employees' Training

The Company shall have an ongoing employee training program so that the members of the Company are adequately trained in KYC/AML procedures and fully understand the rationale behind the KYC/AML policies and implement them consistently.

All necessary circulars, guidelines, notifications issued by the RBI or government authority in connection with KYC / AML procedures will be communicated to all relevant members of the Company by the Compliance Officer. Relevant members of the Company shall include frontline staff, back-office staff, senior staff, risk management staff and staff dealing with new clients. The training shall include all frontline staff, operations staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policy of Ambium, regulation and related issues shall be ensured by the compliance officer.

iv. **Customer Education:** The Company may prepare specific literature/ pamphlets etc. to educate the customer of the objectives of the KYC programme. The Company on an ongoing basis educates the front desk staff, the branch staff, and the new joiners on the elements of KYC through various training programs.

IX. POLICY REVIEW

The Board of Directors shall review this Policy annually or on a need-basis i.e., in the event of change in regulatory framework or for business or operational need (whichever is earlier). Such updates / changes to the Policy will be communicated to the relevant staff /personnel (both in-house or outsourced) and relevant stakeholders across the Company.

X. COMPLIANCE WITH POLICY

For transactions undertaken, implementation of the principles of this Policy shall be maintained as

follows: (i) the leading credit/risk associate shall be the maker for the conformity with the Policy;

(ii) Post the maker review, any member of the Executive Committee of the Board of Directors, or any such person as may be authorized by the Board shall confirm the compliance with the Policy as checker.

ANNEXURE 1

CUSTOMER DOCUMENTS (If individual)

A Copy of the following Documents needs to be accompanied with each Loan Application and the same should be authenticated by the Loan Advisors

i. ID Proof (any 1)

a) Ration card with Photo
b) Voter ID
c) PAN Card
d) Passport
e) Driving license
f) Bank passbook with photograph
g) Company ID Card
h) Aadhar Card

ii. Current Residence/Business Address Proof (any 1)

a) Sale deed / registration certificate
b) Utility bills - Electricity Bill (up to 6 months old) or Water Bill or Gas bill
c) Rental / lease agreement
d) Proof of Residence issued by Local Authorities (Municipal Corporation or Gram Panchayat) e) Voter ID
f) Ration card with Photo
g) Passport
h) Driving license
i) Bank Pass Book with Photo
j) Letter from employer (Govt.)
k) Letter from Pradhan (Gram Panchayat) / Counsellor (Zila Parishad/ Municipal).
l) Aadhar Card

iii. Age Proof (any 1)

a) Ration Card
b) Voter ID
c) Passport
d) School Leaving Certificate (SSLC certificate)
e) PAN Card

f) Aadhar Card

iv. **Photographs**

a) Borrower -1
b) Co-borrower-1
c) Guarantor -1 (If applicable)

v. **Financial Documents**: Bills/Income Proof/certificate
vi. **Bank Statements Bank's** updated passbook or bank statement showing transactions of the past 6 months. (Borrower or Co-Borrowers)

ANNEXURE 2

Indicative List for risk categorization Medium & High-Risk Category

Customers that are likely to pose a higher-than-average risk may be categorized as medium or high risk depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples of medium risk category customers are:

1. Non-Resident customers
2. High Net worth Individuals
3. Trust, charities, NGOs, and Organization receiving donations
4. Companies having close family shareholding or beneficial ownership
5. Firms with 'sleeping partners'

Illustrative examples of high-risk category customers are:

1. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
2. Non-face-to-face customers
3. Those with dubious reputation as per public information available
4. Accounts of bullion dealers and Jewellers 2
5. Property dealers
6. Customers dealing with arms and ammunition
7. Customer is in speculation business

Indicative List for risk categorization Low Category

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile and not covered in any of the above two categories, shall be categorized as low risk.

Illustrative examples of Low-risk category customers are:

1. Salaried employees whose salary structure is well-defined
2. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
3. Government departments and Government-owned companies
4. Statutory bodies & Regulators

wint CAPITAL

END OF DOCUMENT

This document is the property of Ambium Finserve Limited.