



FLAT WHITE CAPITAL PRIVATE LIMITED

*(A Non-Banking Financial Company – Investment and Credit Company
(NBFC-ICC) Registered with Reserve Bank of India)*

**KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY
LAUNDERING (AML) POLICY**

**Document No.:** FWCPL/POL/005**Version:** 1**Effective Date:** 13.07.2026**Approved By:** Board of Directors**Policy Owner:** Compliance Department**Review Frequency:** Annual or earlier if required pursuant to any change in applicable law, RBI directions or business requirements.**DOCUMENT CONTROL**

Particular	Details
Document Name	KYC & AML Policy
Document Number	FWCPL/POL/005
Version	1
Policy Owner	Compliance Department
Prepared and Reviewed By	Company Secretary/Finance Head
Approved By	Board of Directors
Effective Date	13.07.2026
Review Frequency	Annual or earlier if required by RBI
Applicable To	All Employees, Branches, Business Correspondents (if any), Service Providers and Customers

APPROVAL MATRIX

Activity	Responsibility
Drafting	Compliance
Business Review	Business & Product Team
Legal Review	Legal Department
Operational Review	Operations Department
Approval	Board of Directors



1. INTRODUCTION AND BACKGROUND:

Flat White Capital Private Limited ("**FWCPL**" or the "**Company**"), a Non-Banking Financial Company – Investment and Credit Company ("NBFC-ICC") registered with the Reserve Bank of India ("RBI"), is committed to maintaining the highest standards of integrity, transparency and regulatory compliance in all its business activities. The Company recognises that effective customer identification and robust anti-money laundering controls constitute the cornerstone of a sound risk management framework and are essential to safeguard the financial system against misuse for money laundering, terrorist financing, proliferation financing and other unlawful activities.

The Company shall maintain and implement a comprehensive Know Your Customer ("KYC") and Anti-Money Laundering ("AML") framework to identify and verify the identity of customers, understand the nature and purpose of customer relationships, assess customer risk, monitor transactions on an ongoing basis and report suspicious activities to the appropriate regulatory authorities wherever required. The framework established under this Policy is intended to ensure that the Company's products and services are not knowingly used for activities prohibited under applicable law.

This Policy has been formulated in accordance with the provisions of the Reserve Bank of India Act, 1934, the Prevention of Money Laundering Act, 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the RBI Master Direction – Know Your Customer (KYC) Direction, 2016, as amended from time to time, the RBI Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023, as amended, and all other applicable circulars, notifications, guidelines and directions issued by the Reserve Bank of India, Financial Intelligence Unit – India ("FIU-IND") and other competent authorities.

The provisions of this Policy shall be binding upon all Directors, employees, officers and authorised representatives of the Company. Every person associated with customer onboarding, credit appraisal, operations, compliance, technology, collections and customer servicing shall ensure strict adherence to the requirements contained herein.

BACKGROUND:

The term 'Money Laundering' refers to act of concealing or disguising origin and ownership of proceeds from criminal activities including drug trafficking, public corruption, terrorism, fraud, human trafficking and organized crime activities. 'Terrorist Financing' is the use of legally or illegally obtained funds to facilitate terrorist activities. 'Money Laundering' and 'Terrorist Financing' may involve a wide variety of financial products, services and transactions including lending & investment products, financing of equipment or other property that could be used to facilitate terrorism and other criminal activity.

Almost every crime with a profit motive can create proceeds that can be laundered. For example, fraud, theft, illegal drug sales, organized crime, bribery, corruption of government officials and human trafficking can create illegal funds that a criminal seeks to convert into legitimate property without raising suspicion. Tax evasion and violations of fiscal laws can also lead to money laundering.

Generally, the process of Money Laundering involves three stages, viz.

(i) Placement; (ii) Layering; and (iii) Integration. As illegal funds move from the placement stage to the integration stage, it becomes increasingly harder to detect and trace back to the illegal source.

- **Placement** is the point where illegal funds first enter the financial system. The deposit of illegal cash into an account or the purchase of money orders, cashier's checks or other financial product is made. Non-bank financial institutions, such as currency exchanges, money remitters, casinos, and check-cashing services can also be used for placement.
- **Layering** After illegal funds have entered the financial system, layers are created by closing and opening accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.
- **Integration** occurs when the criminal believes that there are sufficient number of layers hiding the origin of the illegal funds to safely invest the funds or apply them towards purchasing valuable property in the legitimate economy.

A financial institution or other business may be used at any point in the process of money laundering. The criminals and other anti-social elements keep coming-up with innovative means to launder money and no financial institution or business is immune from possible victimization.

To address issue of money laundering, the Government of India and other countries around the world have made money laundering a crime and prescribed regulatory requirements for compliance by the banks, financial companies/ institutions and other regulated/ reporting entities to prevent and detect money laundering.

To prevent money-laundering in India and to provide for confiscation of property derived from or involved in money-laundering and related matters, the Government of India enacted the Prevention of Money Laundering Act, 2002(PMLA),as amended from time to time. Further, the PMLA and necessary Notifications/ Rules there under have been published and amended thereafter.

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

Further, "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."

The PMLA and the Rules notified there under impose obligation on banking companies, financial institutions (which includes chit fund Company, a co-operative bank, a non- banking financial company and a housing finance institution) and other defined intermediaries to verify identity of clients, maintain records and furnish requisite information to Financial Intelligence Unit- India (FIU-IND). The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

The KYC and AML Policy has been prepared considering the following key elements:

- a) To lay down the criteria for Customer Acceptance(CAP);
- b) Risk Management;
- c) To lay down criteria for Customer Identification Procedures(CIP);
- d) To establish procedures for monitoring of transactions as may be applicable;

2. PURPOSE:

The purpose of this Policy is to establish a comprehensive framework governing customer onboarding, customer identification, customer due diligence, enhanced due diligence, ongoing monitoring of customer relationships, reporting of suspicious transactions and compliance with the anti-money laundering obligations applicable to the Company.

The Policy seeks to minimise the risk of the Company being used, intentionally or unintentionally, for money laundering, terrorist financing, proliferation financing or any other financial crime. It also aims to protect the Company against legal, regulatory, operational and reputational risks while ensuring that legitimate customers receive financial services through a fair, transparent and efficient onboarding process.

This Policy further lays down the principles governing customer due diligence, risk classification, record maintenance, regulatory reporting, internal monitoring and employee responsibilities so as to promote a culture of compliance throughout the organisation.

3. SCOPE & APPLICABILITY:

This Policy shall apply to all business operations, products and services offered by the Company, including all Gold Loan products and any other financial products or services that may be introduced by the Company in future.

The Policy shall be applicable to every branch, business location, digital platform or its related product or application, employee, officer, director and authorised representative of the Company. It shall also extend to service providers or technology partners performing customer onboarding, CKYC registration, identity verification or other KYC-related activities on behalf of the Company, provided that the ultimate responsibility for compliance with the applicable regulatory requirements shall continue to rest with the Company.

The provisions of this Policy shall govern the entire customer lifecycle, including customer onboarding, customer identification, periodic updation of KYC records, monitoring of customer transactions, reporting of suspicious activities, preservation of records and termination of customer relationships, wherever necessary.

This Policy shall be effective from the date of approval of this policy. The Policy shall be reviewed as and when required by the applicable rules and regulations. The Policy and any significant changes therein shall be approved by the Board of Directors of the Company.

4. REGULATORY FRAMEWORK:

This Policy has been formulated in accordance with the provisions of the Reserve Bank of India Act, 1934, the Prevention of Money Laundering Act, 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the RBI Master Direction – Know Your Customer (KYC) Direction, 2016, the RBI Master Direction – Know Your Customer (KYC) Direction, 2025 (updated as on 29th December 2025) as amended from time to time, the RBI Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023, as amended from time to time, and other applicable circulars, notifications, guidelines and directions issued by the Reserve Bank of India ("RBI"), Financial Intelligence Unit – India ("FIU-IND"), Central Registry of Securitisation Asset Reconstruction and Security Interest of India ("CERSAI"), Central KYC Records Registry ("CKYCR") and other statutory or regulatory authorities.

The Company shall ensure continuous compliance with all applicable regulatory requirements governing customer identification, customer due diligence, beneficial ownership, anti-money laundering measures, countering the financing of terrorism, record maintenance, regulatory reporting and ongoing monitoring of customer relationships. The Compliance Department shall monitor regulatory developments and recommend suitable amendments to this Policy to ensure that the Company's KYC and AML framework remains aligned with the prevailing legal and regulatory requirements.

Where any provision of this Policy is inconsistent with any applicable law, regulation or regulatory direction, the applicable legal or regulatory requirement shall prevail to the extent of such inconsistency. Necessary amendments to this Policy shall thereafter be placed before the Board of Directors for approval at the earliest opportunity.

The Company may issue operational procedures, standard operating procedures ("SOPs"), circulars, guidance notes and internal instructions from time to time for effective implementation of this Policy. Such operational documents shall be read in

conjunction with this Policy and shall not dilute the requirements prescribed under the applicable regulatory framework.

5. DEFINITIONS:

Unless the context otherwise requires, the following expressions shall have the meanings assigned to them below. Words and expressions not specifically defined in this Policy shall have the meanings assigned to them under the applicable laws, RBI Directions or PMLA.

"Beneficial Owner" means the natural person(s) who ultimately own, control or have a controlling ownership interest in a customer or on whose behalf a transaction is conducted and shall have the meaning assigned under the applicable provisions of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the RBI Master Direction – Know Your Customer (KYC) Direction, as amended from time to time.

"Central KYC Records Registry (CKYCR)" means the central repository established under the Prevention of Money Laundering Rules for receiving, storing, safeguarding and retrieving KYC records in electronic form.

"Customer" means a person who establishes or intends to establish a business relationship with the Company, applies for or avails any financial product or service, or otherwise required to comply with the Company's KYC requirements under applicable law and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

"Customer Due Diligence (CDD)" means the process of identifying and verifying the identity of the customer and the beneficial owner, understanding the nature and purpose of the business relationship, assessing customer risk and undertaking ongoing monitoring of the customer relationship in accordance with the applicable regulatory framework.

"Cash Transaction Report (CTR)" CTR will include the following:

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

"Designated Director" means the Director designated by the Board of Directors in accordance with the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder for ensuring overall compliance with the obligations prescribed under the applicable money laundering framework and includes:-

- a) the Managing Director or a whole-time Director or director duly authorized by the Board,
- b) A person of senior management official designated by the Company as "Designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012.

However, in no case, the Principal Officer should be nominated as the "Designated Director".

"Officially Valid Document (OVD)" shall have the meaning assigned under the RBI Master Direction – Know Your Customer (KYC) Direction and includes such documents as may be notified by the Reserve Bank of India or the Central Government from time to time for establishing the identity and address of a customer.

"Politically Exposed Person (PEP)" means an individual who is or has been entrusted with prominent public functions in India or in a foreign jurisdiction and shall include persons as recognised under the applicable regulatory framework.

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

"Senior Management" for the purpose of KYC compliance shall include members of the Executive Committee, Designated Director, Principal Officer (PO) and his supervisor.

"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 the proceeds of crime, regardless of the value involved; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or

- c) appears to have no economic rationale or bona fide purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

“Transaction” - means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- a) opening of an account;
- b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- c) 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 of any contractual or other legal obligation;
- f) establishing or creating a legal person or legal arrangement.

7. GOVERNANCE FRAMEWORK:

The Company shall establish and maintain an effective governance framework to ensure implementation of this Policy across all business functions. The governance framework shall clearly define the roles, responsibilities and accountability of the Board of Directors, Designated Director, Principal Officer, Senior Management, Compliance Department, Operations Department and all employees responsible for customer onboarding and account management.

The governance framework shall ensure that adequate systems, internal controls, technology infrastructure and monitoring mechanisms are established to effectively identify, assess, monitor and mitigate money laundering, terrorist financing and other financial crime risks associated with the Company's business activities.

The Company shall adopt a risk-based approach for implementation of this Policy and shall ensure that adequate resources are deployed for effective compliance with the applicable regulatory requirements. The governance framework shall be reviewed

periodically to ensure its continued effectiveness and alignment with regulatory expectations.

7.1 Role of the Board of Directors

The Board of Directors shall have the overall responsibility for approving this Policy and ensuring that the Company maintains an effective KYC and AML framework in accordance with the applicable regulatory requirements.

The Board shall periodically review the implementation of this Policy and satisfy itself that adequate internal controls, governance arrangements, technology systems and compliance mechanisms are in place to identify and mitigate money laundering and terrorist financing risks.

The Board shall ensure that appropriate policies, procedures and operational controls are established for customer onboarding, customer due diligence, risk classification, transaction monitoring, record maintenance and regulatory reporting. The Board shall also review material compliance observations, significant AML incidents, regulatory inspection findings and corrective actions placed before it by the Compliance Department or the Principal Officer.

The Board may delegate operational responsibilities to designated officials; however, such delegation shall not dilute the Board's overall responsibility for ensuring compliance with the applicable regulatory framework.

7.2 Role of the Designated Director

The Company has appointed a Designated Director in accordance with the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder. The Designated Director shall be responsible for ensuring overall compliance with the Company's obligations under the applicable anti-money laundering framework.

The Designated Director shall provide strategic oversight over the Company's AML programme and shall ensure that appropriate governance arrangements, reporting mechanisms and compliance controls are established and maintained. The Designated Director shall periodically review significant AML risks, regulatory developments and compliance reports submitted by the Principal Officer and the Compliance Department.

The Designated Director shall also ensure that adequate resources are available for implementation of this Policy and that corrective actions are taken promptly in respect of any deficiencies identified during internal audit, regulatory inspection or compliance reviews.

7.3 Role of the Principal Officer

The Company shall designate a Principal Officer who shall be responsible for day-to-day implementation of the Company's KYC and AML framework and for ensuring compliance with the reporting obligations prescribed under the Prevention of Money Laundering Act, 2002 and the applicable regulatory directions.

The Principal Officer shall monitor compliance with this Policy, oversee customer due diligence processes, supervise transaction monitoring systems, evaluate suspicious activities, coordinate with FIU-IND and other competent authorities and ensure timely filing of Suspicious Transaction Reports and such other regulatory reports as may be required under applicable law.

The Principal Officer shall maintain appropriate records relating to AML compliance, coordinate employee awareness programmes, support internal audit reviews and periodically submit compliance reports to the Designated Director and the Board of Directors.

7.4 Role of the Compliance Department

The Compliance Department shall act as the custodian of this Policy and shall be responsible for monitoring compliance with the applicable KYC and AML requirements across the organisation.

The Department shall continuously monitor regulatory developments issued by RBI, FIU-IND and other competent authorities and recommend amendments to this Policy wherever necessary. It shall also conduct periodic compliance reviews, identify areas requiring improvement and coordinate implementation of corrective actions.

The Compliance Department shall provide guidance to various business functions on interpretation of regulatory requirements and shall assist in resolving KYC and AML related compliance issues arising during customer onboarding and account servicing.

7.5 Role of Business, Operations and Product Teams

The Business, Operations and Product Teams shall ensure that no customer relationship is established unless all applicable KYC requirements prescribed under this Policy have been satisfactorily completed.

The Operations Team shall verify that customer identification documents, declarations and due diligence requirements have been completed before loan disbursement. The Product and Technology Teams shall ensure that the digital onboarding systems, CKYC integration, customer screening tools and transaction monitoring mechanisms are configured in accordance with applicable regulatory requirements and the operational procedures approved by the Company.

Any exception observed during customer onboarding or account servicing shall immediately be escalated to the Compliance Department for appropriate guidance and resolution.

7.6 Role of Internal Audit

The Internal Audit function, if applicable, shall independently review the adequacy and effectiveness of the Company's KYC and AML framework at periodic intervals. The audit shall evaluate compliance with this Policy, effectiveness of customer due diligence procedures, quality of KYC documentation, CKYC compliance, transaction monitoring systems, regulatory reporting processes and implementation of corrective actions arising from previous audit observations.

Material deficiencies identified during the audit shall be reported to the Board of Directors or the appropriate management authority together with recommendations for corrective action. The concerned departments shall ensure timely implementation of all agreed corrective measures.

8. CUSTOMER ACCEPTANCE POLICY:

The Company shall establish and implement a comprehensive Customer Acceptance Policy to ensure that customer relationships are established only after completion of appropriate due diligence and in accordance with the applicable regulatory requirements. The Customer Acceptance Policy shall form an integral part of the Company's overall KYC and AML framework and shall be implemented uniformly across all business locations, delivery channels and customer onboarding platforms.

The Company shall adopt a risk-based approach while accepting customers and shall ensure that adequate due diligence measures are undertaken commensurate with the risk associated with the customer, the nature of the proposed business relationship, the products and services sought to be availed and the delivery channel used for onboarding. Customer acceptance decisions shall be based on objective



criteria and shall not discriminate against any person on the grounds of religion, caste, gender, marital status, disability or any other prohibited ground under applicable law.

The Company shall not establish or continue any business relationship where it is unable to comply with the applicable customer due diligence requirements or where the identity of the customer or beneficial owner cannot be satisfactorily established and verified. In such cases, the Company may decline the customer relationship or terminate an existing relationship after following the applicable regulatory requirements and internal procedures.

The Company shall ensure that no anonymous account, fictitious account or account in a false or assumed name is opened or maintained. Every customer relationship shall be established only after obtaining the prescribed customer information, completing the applicable KYC verification process and satisfying itself regarding the identity of the customer and the legitimacy of the proposed business relationship.

The Company shall collect only such information and documentation as may be reasonably necessary to comply with the applicable legal and regulatory requirements and to assess the risk associated with the customer relationship. The Company shall endeavour to ensure that the customer onboarding process remains simple, transparent and convenient while maintaining compliance with the applicable KYC and AML obligations.

Where the Company is unable to complete the prescribed Customer Due Diligence ("CDD") requirements before commencement of the business relationship, the Company shall not disburse any loan, create any customer relationship or permit any transaction unless otherwise permitted under the applicable regulatory framework.

If applicable, the Company shall identify customers requiring Enhanced Due Diligence ("EDD") based on the risk assessment framework adopted by the Company. Customers identified as high-risk, including Politically Exposed Persons ("PEPs"), non-resident customers, legal entities with complex ownership structures or such other categories as may be identified under the Company's risk management framework, shall be subjected to enhanced verification, additional documentation and appropriate approval before establishing the business relationship.

The Company shall reserve the right to decline any customer relationship where the information or documents furnished by the customer are found to be false, misleading, inconsistent or incapable of independent verification, or where the



proposed relationship exposes the Company to unacceptable legal, regulatory, reputational or financial crime risks.

The Company shall periodically review customer relationships and customer risk profiles to ensure that the information available with the Company remains complete, accurate and up to date. Appropriate action shall be taken where deficiencies are identified during periodic review or ongoing monitoring.

Any exception to the Customer Acceptance Policy shall be permitted only with the prior approval of the competent authority designated by the Company and shall be appropriately documented together with the reasons for granting such exception. All such exceptions shall be subject to periodic review by the Compliance Department.

9. CUSTOMER IDENTIFICATION PROCEDURE (CIP):

The Company shall establish and maintain a Customer Identification Procedure to verify the identity of every customer before establishing a business relationship or disbursing any loan. The identification process shall be carried out in accordance with the applicable provisions of the RBI Master Direction – Know Your Customer (KYC) Direction, the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder.

Customer identification shall include verification of the customer's identity, proof of address, Permanent Account Number ("PAN") or Form 60, Officially Valid Documents ("OVDs"), photograph, mobile number, e-mail address, CKYC identifier, where available, and such other information as may be required under the applicable regulatory framework or the Company's internal procedures.

The Company may undertake customer identification through physical verification, digital onboarding, CKYC records, Video-based Customer Identification Process or such other legally permissible modes as may be adopted by the Company from time to time in accordance with the applicable regulatory framework.

The Company shall ensure that customer identification is completed prior to loan sanction and disbursement and that all records obtained during the identification process are maintained in a secure manner for the period prescribed under applicable law.

10. CUSTOMER DUE DILIGENCE (CDD):

10.1 General

The Company shall undertake Customer Due Diligence ("CDD") before establishing any business relationship, sanctioning or disbursing any credit facility, carrying out any transaction for a customer or undertaking any activity requiring compliance under the applicable regulatory framework. The objective of Customer Due Diligence shall be to identify and verify the identity of the customer and, wherever applicable, the beneficial owner, understand the nature and purpose of the proposed business relationship, assess the money laundering and terrorist financing risks associated with the customer and ensure that such risks are appropriately managed throughout the duration of the customer relationship.

The extent of Customer Due Diligence to be carried out by the Company shall be commensurate with the risk profile of the customer and the nature, complexity and value of the proposed transaction. The Company shall adopt a risk-based approach and may require additional information or documentation where considered necessary for effective risk assessment.

10.2 Identification and Verification of Individual Customers

Before establishing a business relationship with an individual customer, the Company shall identify and verify the identity of the customer using reliable, independent and authentic documents, data or information in accordance with the applicable regulatory framework.

The Company shall obtain and verify such information as may be prescribed under the applicable RBI Directions, including the customer's full name, date of birth, photograph, Permanent Account Number (PAN) or Form 60, Officially Valid Documents (OVDs), current address, mobile number, e-mail address, occupation and such other information as may be considered necessary for establishing the identity of the customer and assessing the associated risk.

Where the customer has already completed KYC and has provided a valid KYC Identifier, the Company may retrieve the KYC records from the Central KYC Records Registry (CKYCR) in accordance with the applicable regulatory framework and may rely upon such records after carrying out such verification as may be considered appropriate.

10.3 Customer Due Diligence for Sole Proprietorship

In the case of a sole proprietorship, the Company shall carry out Customer Due Diligence of the proprietor and obtain documentary evidence establishing the existence of the proprietary concern in accordance with the applicable RBI Directions. The Company may obtain such registrations, licences, tax registrations, utility bills or other documents evidencing the business activity of the proprietary concern. Where permitted by RBI, the Company may accept an alternative combination of documents after undertaking appropriate verification of the business activity and the existence of the proprietary concern.

10.4 Customer Due Diligence for Legal Entity

Where the customer is a company, partnership firm, limited liability partnership, trust, society or any other juridical person, the Company shall undertake appropriate due diligence to establish the legal existence of the entity, identify and verify the persons authorised to act on its behalf and identify the beneficial owner in accordance with the applicable provisions of the Prevention of Money Laundering Act, the Rules framed thereunder and the RBI Master Direction – Know Your Customer (KYC) Direction.

The Company shall obtain constitutional documents, authorisations, beneficial ownership information and identity documents of authorised signatories in accordance with the constitution of the legal entity. Depending upon the nature of the customer, the Company shall obtain documents including the Certificate of Incorporation, Memorandum and Articles of Association, Partnership Deed, LLP Agreement, Trust Deed, Registration Certificate, PAN, Board Resolution, Power of Attorney and such other documents as may be prescribed under the applicable regulatory framework to establish the legal existence of the customer and identify the persons authorised to act on its behalf.

10.5 Beneficial Ownership

The Company shall identify and verify the Beneficial Owner ("BO") in every case where the customer is a legal person or where the ownership or control structure requires such identification under the applicable regulatory framework.



Reasonable measures shall be taken to understand the ownership and control structure of the customer and to identify the natural person(s) who ultimately own or control the customer or on whose behalf the transaction is being conducted.

Where the Company is unable to identify or verify the beneficial owner or is not satisfied with the ownership structure of the customer, it may decline to establish the proposed business relationship or may terminate an existing relationship in accordance with applicable law and internal procedures.

10.6 Purpose and Nature of Business Relationship

The Company shall obtain sufficient information to understand the purpose and intended nature of the proposed business relationship. Such information shall enable the Company to determine whether the proposed transaction is consistent with the customer's profile, source of funds, occupation, financial position and the products or services sought to be availed.

Where the information available indicates an unusually complex, inconsistent or suspicious transaction pattern, the Company may seek additional information, conduct enhanced due diligence or decline the proposed relationship, as considered appropriate.

10.7 KYC Validity on Branch Transfer

Where the customer relationship is transferred from one branch, office or business location of the Company to another, the KYC verification already completed by the Company shall continue to remain valid, provided that the KYC records are complete and are not due for periodic updation.

10.8 Completion of Customer Due Diligence

Customer Due Diligence shall ordinarily be completed before establishing the business relationship or disbursing any loan. No Gold Loan shall be disbursed unless the prescribed KYC requirements have been satisfactorily completed, except where specifically permitted under the applicable regulatory framework.

Where deficiencies are observed in the information or documentation furnished by the customer, the Company shall require the customer to rectify such deficiencies before proceeding with the proposed transaction.

If the Company is unable to complete Customer Due Diligence within the prescribed time or is unable to satisfy itself regarding the identity of the customer, the Company may decline the application, suspend processing of the transaction or discontinue the business relationship, as may be appropriate.

10.9 Reliance on Third Parties

The Company may, where permitted under the applicable regulatory framework, rely upon Customer Due Diligence carried out by a regulated third party, provided that such reliance does not absolve the Company of its responsibility for compliance with the applicable KYC and AML requirements.

The Company shall ensure that all information and records obtained from such third party are available without undue delay and that the third party is itself regulated, supervised and compliant with the applicable KYC and AML requirements.

11. ENHANCED DUE DILIGENCE (EDD):

The Company shall apply Enhanced Due Diligence ("EDD") measures in respect of customer relationships, products, delivery channels or transactions that are assessed as presenting a higher risk of money laundering, terrorist financing or other financial crime. The extent of enhanced due diligence shall be commensurate with the level of risk identified and shall be undertaken in addition to the standard Customer Due Diligence requirements prescribed under this Policy.

The Company shall identify high-risk customers through its risk assessment framework by considering factors including the customer's profile, occupation, source of funds, nature of business, geographical location, transaction behaviour, ownership structure, mode of onboarding and any other risk indicators considered relevant by the Company. Enhanced Due Diligence shall also be undertaken where required under the applicable regulatory framework or where the Company considers such measures necessary for prudent risk management.

Enhanced Due Diligence may include obtaining additional identity documents, verifying the source of funds and source of wealth, obtaining additional information regarding the purpose of the proposed business relationship, conducting independent verification from reliable sources, obtaining approvals from the designated approving authority and subjecting the customer relationship to enhanced ongoing monitoring. Where the Company is not satisfied with the information obtained during the Enhanced Due Diligence process or where the customer fails to provide the additional

information or documents sought by the Company, the Company may decline the proposed business relationship or discontinue an existing relationship in accordance with applicable law and internal procedures.

12. CUSTOMER RISK CATEGORISATION:

The Company shall adopt a risk-based approach for categorising customers based on the degree of money laundering, terrorist financing and reputational risk associated with the customer relationship. Customer risk categorisation shall be carried out at the time of onboarding and shall be reviewed periodically throughout the duration of the customer relationship.

For the purpose of risk assessment, customers shall ordinarily be classified into Low Risk, Medium Risk and High Risk categories based upon the Company's approved risk assessment methodology. The categorisation shall take into consideration various factors including the nature of the customer, occupation, source of income, geographical location, ownership structure, transaction pattern, mode of onboarding, delivery channel, product type and such other parameters as may be determined by the Company from time to time.

Risk categorisation shall not be based solely upon the volume of business or profitability of the customer relationship. The Company shall ensure that every customer is subjected to an objective and documented risk assessment process.

The customer risk classification may be revised where significant changes are observed in the customer's profile, transaction behaviour, source of funds, ownership structure or any other material information relevant to the Company's risk assessment.

High-risk customer relationships shall be subject to enhanced monitoring and periodic review by the Compliance Department and such other officials as may be authorised by the Company.

13. POLITICALLY EXPOSED PERSONS :

The Company shall if applicable, establish appropriate procedures for identifying customers who are Politically Exposed Persons or are connected with PEPs, in accordance with the applicable regulatory framework.

Where a customer is identified as a PEP, the Company shall undertake Enhanced Due Diligence before establishing the business relationship. The Company shall obtain approval from the appropriate senior management authority prior to onboarding such customer and shall take reasonable measures to establish the source of wealth, source of funds and legitimacy of the proposed business relationship.

The Company shall subject all customer relationships involving PEPs to enhanced ongoing monitoring throughout the duration of the relationship. Where an existing customer subsequently becomes a PEP, the Company shall undertake an appropriate review of the relationship and implement enhanced due diligence measures as considered necessary.

The Company may decline or discontinue any customer relationship involving a PEP where the associated risks cannot be satisfactorily mitigated or where the customer fails to comply with the Company's due diligence requirements.

14. BENEFICIAL OWNERSHIP:

The Company shall identify and verify the Beneficial Owner in respect of all legal persons, juridical entities and such other customers as may be prescribed under the applicable regulatory framework. The identification of the Beneficial Owner shall be carried out in accordance with the Prevention of Money Laundering Act, the Rules framed thereunder and the RBI Master Direction – Know Your Customer (KYC) Direction, as amended from time to time.

The Company shall obtain sufficient information to understand the ownership and control structure of the customer and identify the natural person or persons who ultimately own, control or exercise effective control over the customer or on whose behalf the transaction is being conducted.

Where the ownership structure is complex, layered or otherwise difficult to understand, the Company may obtain additional declarations, constitutional documents or independent verification before establishing the business relationship. Where the Company is unable to identify or verify the Beneficial Owner to its satisfaction, or where the ownership structure gives rise to concerns relating to money laundering or terrorist financing, the Company may decline to establish the proposed relationship or terminate an existing relationship in accordance with applicable law and internal procedures.

15. VIDEO-BASED CUSTOMER IDENTIFICATION PROCESS:

The Company may onboard customers through digital or non-face-to-face channels, including the Video-based Customer Identification Process, where such onboarding is permitted under the applicable regulatory framework and has been operationally implemented by the Company.

The Company shall ensure that digital onboarding processes incorporate adequate technological, operational and security controls to establish the identity of the customer, prevent identity fraud, maintain the integrity of customer records.

Where customers are onboarded through non-face-to-face modes, the Company may apply additional due diligence measures, including enhanced verification, additional authentication procedures, liveness detection, geo-tagging, device verification, video interaction or such other controls as may be considered appropriate by the Company. The Company shall ensure that the technology platforms used for digital onboarding maintain appropriate audit trails, data integrity, information security and record preservation standards.

Where the Company implements the Video-based Customer Identification Process, the process shall be conducted strictly in accordance with the applicable RBI Directions. The authorised official conducting the V-CIP shall perform live interaction with the customer, capture audio and video recordings, obtain a live photograph and verify the identity of the customer using the modes permitted under the applicable regulatory framework.

The Company shall ensure that PAN or e-PAN details are independently verified from the issuing authority, Aadhaar information is appropriately masked wherever required, equivalent e-documents obtained through DigiLocker or other legally recognised platforms and all V-CIP records are securely stored within India together with complete audit logs and date-time stamps.

Where the customer is identified using Aadhaar XML or Aadhaar Secure QR Code, the Company shall ensure compliance with the validity period prescribed by the Reserve Bank of India. The Company shall also ensure that customer accounts opened through V-CIP are subjected to concurrent audit before being made fully operational and that appropriate information security controls are implemented in accordance with applicable law.

16. OFFICIALLY VALID DOCUMENTS:

The Company shall obtain and verify the Officially Valid Documents of every customer in accordance with the applicable provisions of the RBI Master Direction – Know Your Customer (KYC) Direction, as amended from time to time. The identity and address of the customer shall be established only through such documents, information or electronic records as are recognised under the applicable regulatory framework.

Where the customer submits an Officially Valid Document containing the current address, no additional proof of address shall ordinarily be insisted upon. However, where the address mentioned in the Officially Valid Document does not correspond to the customer's present address, the Company may obtain such additional documents or declarations as may be permitted under the applicable regulatory framework for the purpose of establishing the current address.

The Company may accept electronic documents, digitally signed records, documents obtained through CKYCR, Aadhaar based authentication, Video-based Customer Identification Process or such other legally recognised modes of identification as may be permitted by the Reserve Bank of India from time to time. The Company shall ensure that all identification documents obtained during the customer onboarding process are complete, valid, legible and capable of independent verification.

Where any document submitted by the customer appears to be forged, altered, expired, inconsistent or otherwise unreliable, the Company shall undertake additional verification and may decline the proposed customer relationship if the deficiencies cannot be satisfactorily resolved.

17. CENTRAL KYC (CKYC):

The Company shall comply with the requirements relating to the Central KYC Records Registry ("CKYCR") in accordance with the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the applicable directions issued by the Reserve Bank of India from time to time.

Where a customer has already been registered with CKYCR and provides a valid KYC Identifier, the Company may retrieve the KYC records from CKYCR in accordance with the applicable regulatory framework and rely upon such records after carrying out the necessary verification and obtaining any updated information, where required.

For customers who are not registered with CKYCR, the Company shall upload the KYC records to CKYCR within the timelines prescribed under the applicable regulatory framework through its authorised system or designated technology platform. The Company shall ensure that the KYC Identifier generated by CKYCR is communicated to the customer in the manner prescribed under the applicable regulatory requirements.

Where any modification or updation is carried out in the KYC records of an existing customer, the Company shall update the revised records with CKYCR within the prescribed regulatory timelines and maintain appropriate audit trails of such updation.

18. PERIODIC UPDATION OF KYC:

The Company shall undertake periodic updation of customer KYC records in accordance with the risk categorisation of the customer and the applicable regulatory framework. The objective of periodic updation shall be to ensure that the customer information, identity records and risk profile maintained by the Company remain complete, accurate and up to date throughout the customer relationship.

The frequency and extent of periodic KYC updation shall be determined based on the customer's risk classification and such other parameters as may be prescribed by the Reserve Bank of India from time to time. The Company may seek updated identity documents, address proof, contact details, occupation, source of funds or any other information considered necessary for continued compliance with the applicable KYC requirements.

The Company shall make reasonable efforts to notify customers regarding the requirement for periodic KYC updation and provide appropriate channels for submission of updated information. Failure of the customer to comply with such requirements within the prescribed time may result in restrictions on the operation of the customer relationship or such other action as may be permitted under the applicable regulatory framework.

The Company shall undertake periodic updation of KYC records based on the customer's risk categorisation. As a general principle, KYC shall ordinarily be updated 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 or within such timelines as may be prescribed by the Reserve Bank of India from time to time. Where there is no change in KYC information, the Company may obtain an



appropriate self-declaration through such channels as may be permitted under the applicable regulatory framework. Where only the customer's address has changed, the Company may obtain a self-declaration and complete the prescribed verification within the regulatory timelines.

19. ONGOING DUE DILIGENCE AND TRANSACTION MONITORING:

The Company shall maintain systems for identifying large, complex or unusual transactions, transaction patterns inconsistent with the customer's declared profile, unusually high account activity and such other transactions as may indicate potential money laundering or terrorist financing risks. The Company may utilise automated monitoring systems and emerging technologies, including Artificial Intelligence and Machine Learning , wherever considered appropriate, to strengthen transaction monitoring and risk management. High-risk customer relationships shall be subjected to enhanced monitoring and periodic review in accordance with the Company's Risk-Based Approach.

The Company shall continuously monitor customer relationships and transactions throughout the duration of the business relationship to ensure that the transactions undertaken are consistent with the customer's profile, declared source of funds, occupation, financial position and the nature of the products and services availed from the Company.

Appropriate monitoring systems shall be established to identify unusual, inconsistent, complex or high-value transactions that are not commensurate with the customer's known profile or which otherwise give rise to suspicion of money laundering, terrorist financing or any other unlawful activity. Such transactions shall be subjected to appropriate review by the Compliance Department and, where necessary, escalated to the Principal Officer for further examination.

The Company shall apply enhanced monitoring measures to customers classified as High Risk, Politically Exposed Persons (PEPs), legal entities having complex ownership structures, non-face-to-face customers and such other categories of customers as may be identified under the Company's risk assessment framework.

Where the Company identifies any transaction or activity that appears unusual or suspicious, it may obtain additional information from the customer, carry out enhanced due diligence, place appropriate restrictions on the customer relationship or take such other action as may be considered necessary in accordance with applicable law and this Policy.

The Company shall maintain appropriate systems for documenting the outcome of transaction monitoring activities, risk assessments and compliance reviews to facilitate regulatory reporting, audit and supervisory inspection.

20. REPORTING OF SUSPICIOUS TRANSACTIONS:

The Company shall establish and maintain appropriate systems and procedures for identifying, examining and reporting suspicious transactions in accordance with the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and the applicable directions issued by the Reserve Bank of India and the Financial Intelligence Unit – India ("FIU-IND").

Every employee shall remain vigilant while dealing with customers and shall promptly report any unusual, inconsistent, suspicious or potentially fraudulent activity observed during customer onboarding, loan processing, account servicing or any other stage of the customer relationship to the Principal Officer through the prescribed internal reporting mechanism. Employees shall not independently determine whether a transaction constitutes a reportable suspicious transaction but shall immediately escalate such matters for appropriate examination.

The Principal Officer shall examine all internal alerts, determine whether a Suspicious Transaction Report ("STR") or any other report is required to be filed with FIU-IND if applicable and ensure that such reporting is completed within the timelines prescribed under the applicable regulatory framework. The identity of the employee reporting a suspicious activity and the fact that a report has been or may be filed with FIU-IND shall be kept strictly confidential.

The Company shall maintain appropriate documentation relating to suspicious transaction reviews, internal investigations, decisions taken and regulatory reporting for the period prescribed under the applicable legal and regulatory framework.

21. RECORD RETENTION:

The Company shall maintain records relating to customer identification, customer due diligence, account files, business correspondence, transaction records, KYC documents and regulatory reports in accordance with the requirements of the Prevention of Money Laundering Act, 2002, the Rules framed thereunder and the applicable RBI Directions.

All records shall be preserved in a secure manner so as to enable reconstruction of individual transactions and facilitate regulatory inspection, audit, investigation or judicial proceedings whenever required. The Company shall ensure that physical and electronic records remain complete, accurate, retrievable and protected against unauthorised access, alteration or destruction.

Where records are maintained in electronic form, appropriate controls relating to data security, access management, backup, disaster recovery and audit trails shall be implemented to preserve the integrity and confidentiality of such records.

Upon expiry of the applicable statutory retention period, records may be disposed of in accordance with the Company's Record Retention Policy and applicable legal requirements, ensuring that confidential customer information is destroyed securely and cannot be reconstructed or misused.

22. SANCTIONS SCREENING:

The Company shall establish appropriate mechanisms to screen customers, beneficial owners and authorised signatories against sanctions lists, watchlists, regulatory directives and such other databases as may be considered necessary for effective management of money laundering and terrorist financing risks.

Where a customer or transaction matches any applicable sanctions list or gives rise to concerns regarding terrorist financing, proliferation financing or other prohibited activities, the matter shall immediately be escalated to the Principal Officer and the Compliance Department for detailed examination. The Company shall take such action as may be required under applicable law, including suspension of onboarding, enhanced due diligence, reporting to the competent authorities or rejection of the customer relationship, as applicable.

The Company shall periodically review its sanctions screening process and ensure that the databases, screening parameters and technology systems used for such purpose remain updated and effective.

23. EMPLOYEE TRAINING AND AWARENESS:

The Company recognises that an effective KYC and AML framework requires continuous awareness and active participation of all employees. Accordingly, the Company shall conduct periodic training programmes to familiarise employees with the provisions of this Policy, the applicable regulatory framework, emerging money laundering risks, internal reporting procedures and their respective responsibilities. Training programmes shall be conducted at regular intervals and may include induction training for new employees, periodic refresher programmes, role-specific training and updates on regulatory changes issued by the Reserve Bank of India, FIU-IND or other competent authorities.

The Company shall maintain appropriate records of training programmes conducted, attendance of employees and assessment of training effectiveness as part of its compliance monitoring framework.

24. INTERNAL CONTROLS, COMPLIANCE MONITORING AND AUDIT:

The Company shall establish an effective internal control framework to ensure continuous compliance with the provisions of this Policy and the applicable regulatory requirements. Appropriate systems, processes and technology controls shall be implemented to identify deficiencies, monitor compliance and facilitate timely corrective action.

The Compliance Department shall periodically review implementation of this Policy across various business functions and report significant observations to the senior management and the Board of Directors, wherever considered necessary.

The Internal Audit function shall independently evaluate the adequacy and effectiveness of the Company's KYC and AML framework at periodic intervals. The audit shall, inter alia, examine customer onboarding practices, quality of KYC documentation, compliance with customer due diligence requirements, transaction monitoring systems, CKYC compliance, regulatory reporting and implementation of previous audit observations.

All deficiencies identified during compliance reviews or internal audits shall be appropriately documented and corrective actions shall be implemented within the timelines approved by the competent authority.

25. CONFIDENTIALITY AND DATA PROTECTION:

The Company shall maintain strict confidentiality of all customer information obtained during the course of customer identification, due diligence and ongoing monitoring activities. Such information shall be used solely for legitimate business purposes, regulatory compliance and such other purposes as may be permitted under applicable law.

Customer information shall not be disclosed to any third party except where such disclosure is required under applicable law, pursuant to an order of a competent authority, for regulatory reporting, with the consent of the customer or for legitimate business purposes permitted under applicable law.

The Company shall implement appropriate technical and organisational measures to protect customer information against unauthorised access, disclosure, alteration, misuse or loss and shall ensure compliance with the applicable data protection and information security requirements.

26. POLICY REVIEW AND AMENDMENTS:

This Policy shall be reviewed at least annually or earlier whenever considered necessary due to changes in the applicable legal or regulatory framework, changes in the Company's business model, introduction of new products or services, observations arising from regulatory inspections, internal audits or any other material developments affecting the Company's KYC and AML framework.

Any amendment to this Policy shall be placed before the Board of Directors for approval. The Compliance Department shall be responsible for monitoring regulatory developments and initiating appropriate amendments to ensure that this Policy remains consistent with the applicable laws, RBI Directions and industry best practices.

Where immediate implementation of any regulatory requirement becomes necessary, the Company may issue appropriate internal instructions or operational guidelines pending formal approval of the revised Policy by the Board of Directors, to the extent permitted under applicable law.

27. CUSTOMER ACCEPTANCE, EXIT AND RESTRICTIONS:

The Company shall establish customer relationships only after satisfying itself regarding the identity of the customer, the purpose of the proposed relationship, the legitimacy of the source of funds and compliance with the requirements prescribed under the applicable regulatory framework.

The Company shall not establish or continue a business relationship where:

- (a) the Company is unable to complete Customer Due Diligence in accordance with this Policy;
- (b) the customer refuses to provide the information or documents required under the applicable legal or regulatory framework;
- (c) the customer provides false, misleading, forged or materially incorrect information;
- (d) the Company has reasonable grounds to suspect that the proposed relationship may involve money laundering, terrorist financing, fraud or any other unlawful activity;
- (e) onboarding or continuation of the relationship is prohibited under any law, regulatory direction, sanctions regime or order of a competent authority.

Where the Company decides not to establish or continue a customer relationship, such decision shall be appropriately documented. The Company may terminate, restrict or suspend the relationship after considering the applicable legal and regulatory requirements and ensuring that such action does not prejudice any investigation or reporting obligation under the Prevention of Money Laundering Act, 2002.

The Company shall ensure that decisions relating to rejection, restriction or termination of customer relationships are based solely upon regulatory, legal, risk management or business considerations and are applied fairly and consistently.

28. POLICY INTERPRETATION:

This Policy shall be read together with the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the RBI Master Direction – Know Your Customer (KYC) Direction, 2016 (as amended from time to time), the Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023 and all circulars, notifications



and instructions issued by the Reserve Bank of India, Financial Intelligence Unit – India and other competent authorities.

In the event of any inconsistency between this Policy and any applicable law or regulatory direction, the provisions of such law or regulatory direction shall prevail to the extent of such inconsistency. The Compliance Department shall initiate appropriate amendments to this Policy for placing before the Board of Directors at the earliest opportunity.

The Compliance Department may issue operational guidelines, standard operating procedures, implementation notes or clarifications consistent with this Policy for facilitating effective implementation across various business functions.

29. EFFECTIVE DATE:

This Policy shall come into force with effect from the date of its approval by the Board of Directors and shall remain in force until amended, modified or superseded.

The Compliance Department shall be responsible for circulating this Policy to all relevant employees, maintaining the latest approved version and ensuring that previous versions are archived in accordance with the Company's document retention procedures.

ANNEXURE – A

CUSTOMER IDENTIFICATION DOCUMENT MATRIX:

The Company shall obtain Customer Due Diligence ("CDD") documents depending upon the constitution of the customer and in accordance with the applicable provisions of the RBI Master Direction – Know Your Customer (KYC) Direction, 2016 (as amended from time to time), the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder. The list of documents set out below represents the minimum documentation requirements. The Company may obtain additional information or documents wherever considered necessary based on the customer's risk profile, product characteristics or regulatory requirements.

A. Individual

For an individual customer, the Company shall obtain and verify the customer's identity and address through an Officially Valid Document ("OVD"), Permanent Account Number (PAN) or Form 60, recent photograph, mobile number, e-mail address (where available), occupation, source of income or source of funds, CKYC Identifier (where available) and such other information as may be considered necessary by the Company. Where the customer has completed KYC through CKYCR or such other legally recognised mechanism, the Company may rely upon such records subject to the applicable regulatory framework.

B. Sole Proprietorship

In addition to the KYC documents of the proprietor, the Company shall obtain documentary evidence establishing the existence of the proprietorship concern, including registrations, licences, tax registrations or such other documents evidencing the business activity of the proprietorship as may be permitted under the applicable RBI Directions.

C. Partnership Firm

The Company shall obtain the Permanent Account Number of the partnership firm, the Partnership Deed, registration certificate (where applicable), authorisation in favour of the person acting on behalf of the firm, KYC documents of all authorised signatories, Beneficial owner documents, list of partners, Registered office and Principal place of business. The Company may obtain additional documents wherever considered necessary to establish the constitution and ownership of the partnership.

D. Limited Liability Partnership (LLP)

The Company shall obtain the Certificate of Incorporation, LLP Agreement, Permanent Account Number, authorisation in favour of authorised signatories, identification documents of designated partners, beneficial ownership declaration and KYC documents of the persons authorised to act on behalf of the LLP.



E. Company

For a company incorporated under the Companies Act, the Company shall obtain the following documents i.e Certificate of Incorporation, Memorandum of Association, Articles of Association, PAN, Board Resolution, Power of Attorney/Authorisation, KYC of authorised signatory, Beneficial Owner documents, List of Senior Management, Registered Office & Principal Place of Business.

F. Trust

The Company shall obtain the Registration Certificate, Trust Deed, PAN/Form 60, Trustees, Settlor, Beneficiaries Protector details (if applicable), BO documents, Registered Office and Trustee KYC together with beneficial ownership information in accordance with the applicable regulatory framework.

G. Society / Association / Club

The Company shall obtain the registration certificate, constitutional documents, Permanent Account Number, resolution authorising the transaction, identity documents of authorised office bearers and beneficial ownership information wherever applicable.

The Company may require any additional information or documentation where considered necessary for effective Customer Due Diligence or where required under the applicable regulatory framework.

ANNEXURE – B
CUSTOMER RISK CATEGORISATION FRAMEWORK:

The Company shall adopt a risk-based approach for categorising customers into Low Risk, Medium Risk and High Risk categories based upon the money laundering, terrorist financing and reputational risks associated with the customer relationship. The customer risk assessment shall consider, inter alia, the customer's identity, occupation, source of income, source of funds, nature of business, geographical location, ownership structure, delivery channel, expected transaction behaviour, product type, mode of onboarding and any adverse information available from reliable public sources.

Customers assessed as High Risk shall be subject to Enhanced Due Diligence, senior management approval (where applicable), enhanced transaction monitoring and more frequent review of KYC records.

The Company shall periodically review customer risk classifications and revise the categorisation wherever there is a material change in the customer's profile, ownership, business activity or transaction behaviour.

ANNEXURE – C

RED FLAG INDICATORS

The Company shall maintain appropriate systems to identify unusual or suspicious activities. The following circumstances may require enhanced scrutiny and, where appropriate, escalation to the Principal Officer:

- Customer refuses or is reluctant to provide KYC information or supporting documents.
- Information provided by the customer is inconsistent, false or incapable of verification.
- Customer attempts to use forged, altered or expired identification documents.
- Frequent changes in customer profile without reasonable explanation.
- Transactions inconsistent with the customer's declared occupation, financial profile or source of funds.
- Multiple transactions structured to avoid regulatory reporting or internal monitoring thresholds.
- Customer demonstrates unusual urgency to complete the transaction without reasonable commercial justification.
- Adverse media reports or information linking the customer with fraud, financial crime or other unlawful activities.
- Any other activity giving rise to reasonable suspicion of money laundering, terrorist financing or fraud.

Identification of a Red Flag Indicator shall not automatically result in rejection of the customer relationship but shall require appropriate examination, documentation and, where necessary, enhanced due diligence.

ANNEXURE – D
BENEFICIAL OWNERSHIP (BO) IDENTIFICATION FRAMEWORK:

The Company shall identify and verify the Beneficial Owner in accordance with Rule 9 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. Appropriate measures shall be taken to understand the ownership and control structure of every legal entity and to identify the natural person(s) exercising ultimate ownership or effective control over the customer.

The Company shall take reasonable measures to identify the natural person(s) who ultimately own, control or exercise effective control over the customer or on whose behalf the transaction is being conducted. The identification of the Beneficial Owner shall be undertaken before establishing the business relationship and shall be periodically reviewed during the course of the relationship.

Where the ownership structure is complex, layered or otherwise difficult to determine, the Company may seek additional declarations, constitutional documents, ownership charts, management information or independent verification to establish the identity of the ultimate beneficial owner.

Where the Company is unable to identify or verify the Beneficial Owner to its satisfaction, or where the ownership structure gives rise to concerns relating to money laundering, terrorist financing or concealment of ownership, the Company may decline the proposed business relationship or discontinue an existing relationship in accordance with applicable law and this Policy.

The Company shall maintain appropriate records of Beneficial Ownership declarations and supporting documents as part of the customer's KYC records.

ANNEXURE – E
PERIODIC KYC UPDATION FRAMEWORK:

The Company shall periodically review and update customer KYC records to ensure that the information maintained by the Company remains accurate, complete and current throughout the customer lifecycle.

The frequency of periodic updation shall be determined on the basis of the customer's risk categorisation and the applicable regulatory framework. The Company may seek updated Officially Valid Documents, address proof, contact details, occupation, source of income, source of funds, beneficial ownership information or such other information as may be necessary to maintain an updated customer profile.

The Company shall establish appropriate mechanisms for notifying customers regarding KYC updation requirements and may facilitate updation through physical, digital or such other legally permissible channels as may be adopted by the Company. Failure by the customer to comply with periodic KYC updation requirements within the prescribed timelines may result in restrictions on the operation of the customer relationship or such other action as may be permitted under the applicable regulatory framework.

All KYC updations shall be appropriately documented and, where applicable, updated with the Central KYC Records Registry (CKYCR) within the prescribed timelines.

ANNEXURE – F
INTERNAL ESCALATION AND REPORTING OF SUSPICIOUS ACTIVITIES:

The Company shall maintain an internal reporting mechanism to facilitate prompt identification, examination and escalation of suspicious transactions or activities. Every employee shall immediately report any unusual, suspicious or potentially fraudulent activity observed during customer onboarding, loan processing, account servicing or any other stage of the customer relationship to the Principal Officer through the prescribed internal reporting process.

Upon receipt of such information, the Principal Officer shall evaluate the available facts, obtain additional information where necessary and determine whether the matter warrants filing of a Suspicious Transaction Report ("STR") or any other report with the Financial Intelligence Unit – India ("FIU-IND") in accordance with applicable law.

All internal investigations, deliberations, supporting documents and decisions relating to suspicious transactions shall be documented and maintained in a confidential manner. Employees shall not disclose to the customer or any unauthorised person that a suspicious transaction report has been or is proposed to be filed with FIU-IND. The Company shall maintain appropriate controls to ensure confidentiality, integrity and timely escalation of suspicious transaction reporting.

ANNEXURE – G

ROLES AND RESPONSIBILITIES:

The Board of Directors shall be responsible for approving the KYC & AML Policy, reviewing its implementation and ensuring that adequate governance and oversight mechanisms are maintained for compliance with the applicable regulatory framework. The Designated Director shall provide overall oversight of the Company's Anti-Money Laundering framework and ensure compliance with the obligations prescribed under the Prevention of Money Laundering Act, 2002 and the Rules framed thereunder.

The Principal Officer shall be responsible for day-to-day administration of the KYC and AML framework, monitoring suspicious transactions, coordinating with FIU-IND, maintaining AML records, ensuring regulatory reporting and providing periodic compliance updates to senior management and the Board.

The Compliance Department shall monitor implementation of this Policy, interpret regulatory requirements, recommend amendments arising from changes in law, conduct compliance reviews and support various business functions in implementation of KYC and AML controls.

The Business, Operations and Product Teams shall ensure compliance with customer onboarding procedures, customer due diligence requirements, CKYC registration, document verification, transaction monitoring controls and such other operational requirements as may be prescribed by the Company.

The Internal Audit function shall independently review the adequacy and effectiveness of the Company's KYC and AML framework and report significant observations together with corrective action recommendations to the appropriate management authority and the Board of Directors.

ANNEXURE – H

REGULATORY REFERENCES

This Policy has been prepared after considering the following principal regulatory framework as amended from time to time:

- Reserve Bank of India Act, 1934.
- Prevention of Money Laundering Act, 2002.
- Prevention of Money Laundering (Maintenance of Records) Rules, 2005.
- RBI Master Direction – Know Your Customer (KYC) Direction, 2016.
- RBI Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023.
- Circulars, notifications, directions and clarifications issued by the Reserve Bank of India relating to Know Your Customer (KYC), Anti-Money Laundering (AML), Countering Financing of Terrorism (CFT), CKYCR, Video-based Customer Identification Process (V-CIP) and related compliance matters.
- Notifications, advisories and reporting requirements issued by the Financial Intelligence Unit – India (FIU-IND).
- Any other applicable law, regulation or regulatory instruction governing customer identification, anti-money laundering or financial crime prevention.

ANNEXURE – I

CUSTOMER RISK ASSESSMENT METHODOLOGY:

The Company shall adopt a comprehensive Risk-Based Approach for assessing and managing the Money Laundering, Terrorist Financing and Proliferation Financing risks associated with every customer relationship. The objective of the risk assessment framework is to ensure that the level of Customer Due Diligence, Enhanced Due Diligence, transaction monitoring and periodic KYC updation undertaken by the Company is commensurate with the risk presented by each customer.

The customer risk assessment shall be performed at the time of onboarding and shall thereafter be reviewed periodically or whenever a material change occurs in the customer's profile, ownership, business activity, transaction behaviour, source of funds or any other factor considered relevant by the Company.

While assigning a customer risk rating, the Company shall consider multiple risk indicators including, but not limited to, the nature of the customer, occupation or business activity, source of income, source of funds, expected account behaviour, geographical location, delivery channel, ownership structure, beneficial ownership, product availed, transaction pattern, regulatory history, adverse media reports and sanctions screening results.

The Company shall classify customers into Low Risk, Medium Risk and High Risk categories based on the overall assessment of the identified risk factors. The methodology adopted for such classification shall be approved by the Board of Directors or such authority as may be authorised by the Board and shall be reviewed periodically to ensure its continued relevance and effectiveness.

The Company may revise the risk category assigned to a customer whenever new information becomes available or where monitoring activities indicate a significant change in the customer's risk profile. Any such revision shall be adequately documented and supported by appropriate justification.



ANNEXURE – J
SANCTIONS, WATCHLIST AND ADVERSE MEDIA SCREENING:

The Company shall establish appropriate systems and controls to identify customers, beneficial owners, authorised signatories and related parties appearing on sanctions lists, watchlists or other databases maintained by competent domestic or international authorities, wherever applicable under law.

The Company shall also undertake appropriate screening against adverse media information, fraud databases and other reliable public sources, wherever considered necessary, for the purpose of identifying potential financial crime risks before establishing or continuing a business relationship.

Where a potential match is identified during sanctions screening or adverse media review, the customer relationship shall not proceed until the matter has been examined by the Compliance Department and the Principal Officer. Appropriate due diligence, verification and documentation shall be completed before any decision is taken regarding acceptance, continuation or rejection of the customer relationship. Where required under applicable law, the Company shall report such matters to the appropriate regulatory or law enforcement authorities and shall implement any restrictions, prohibitions or other measures required under the applicable legal framework.

ANNEXURE – K **EXCEPTION MANAGEMENT:**

The Company recognises that exceptional situations may arise where deviations from the standard customer onboarding process are operationally unavoidable or specifically permitted under the applicable regulatory framework. Such deviations shall be treated as exceptions and shall be subject to appropriate approval, documentation and monitoring.

No exception shall be granted where it would result in violation of any applicable law, RBI Direction, PMLA requirement or regulatory instruction. Business considerations shall not override statutory or regulatory compliance obligations.

Every approved exception shall clearly record the nature of the deviation, reasons for granting the exception, risk assessment performed, mitigating controls implemented, approving authority and validity period of the approval. The Compliance Department shall maintain a central register of all approved KYC and AML exceptions and shall periodically review the same to identify recurring issues requiring policy or process improvements.

Material exceptions shall be placed before the Board of Directors or the appropriate management committee as part of the periodic compliance reporting process.

ANNEXURE – L

POLICY IMPLEMENTATION

The Company shall implement this Policy through appropriate operational procedures, digital systems, internal controls and employee awareness programmes. The Compliance Department shall coordinate with the Operations, Product, Technology, Credit, Risk, Finance and Internal Audit functions to ensure effective implementation of the requirements contained in this Policy.

The Company shall ensure that all technology systems used for customer onboarding, identity verification, CKYC integration, sanctions screening, transaction monitoring and record management are appropriately configured, adequately tested and periodically reviewed to ensure continued compliance with the applicable regulatory framework.

Appropriate Standard Operating Procedures ("SOPs"), operational manuals, user guidelines and system controls may be issued from time to time for effective implementation of this Policy. Such operational documents shall supplement this Policy and shall not dilute or override any requirement prescribed under applicable law or this Policy.

The Company shall periodically assess the effectiveness of the KYC and AML framework through compliance reviews, internal audits, management oversight and regulatory inspections and shall implement appropriate corrective and preventive actions wherever deficiencies are identified.