Anson Fincorp Private Limited

Reg. Office: Door No. XIV/1057, Anson Tower, B. Ed College Junction, Nedumkandam P.O, Nedumkandam, Idukki, Kerala - 685553 India

KNOW YOUR CUSTOMER (KYC) / ANTI MONEY LAUNDERING (AML) POLICY

Version Control		
Version Number	**Description**	**Date**
Version - 1	Approval	01.03.2016
Version -2	Review	02.09.2019
Version – 3	Review	04.05.2020
Version – 4	Review	06.04.2021
Version - 5	Review	24.04.2024
Version -6	Review	30.03.2026

Effective Date	01.04.2026
Prepared by	Secretarial Department
Custodian	Company Secretary
Reviewed by	Board of Directors
Approved by	Board of Directors

1. Introduction

The Reserve Bank of India (RBI) has issued **Reserve Bank of India (Non-Banking Financial Company – Know Your Customer) Directions, 2025**,as amended from time to time, to all Non-Banking Financial Companies (NBFCs) for preventing money laundering, terrorist financing and other financial crimes, in line with the provisions of the Prevention of Money-laundering Act, 2002 (PMLA), the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, and the recommendations of the Financial Action Task Force (FATF).

Accordingly, **Anson Fincorp Private Limited ("AFPL" or "the Company")** has formulated this Know Your Customer (KYC) / Anti-Money Laundering (AML) Policy to ensure compliance with the applicable statutory and regulatory requirements and to establish a robust framework for customer acceptance, customer identification, customer due diligence, ongoing monitoring, reporting of suspicious transactions and risk management.

This Policy has been approved by the Board of Directors of the Company and shall be reviewed periodically or whenever there is any amendment in the applicable laws or RBI Directions.

2. Definitions:

a) A **'Customer'** means a person as defined under KYC Directions of RBI (and any amendment from time to time by RBI) which are at present as under: -

i. A **"Person"** who is engaged in a financial transaction or activity with a company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

b) **AFPL/RE** means Anson Fincorp Private Limited.

c) **KYC** means Know Your Customer

d) **AML** stands for Anti-Money Laundering.

e) **CFT** stands for Combating the Financing of Terrorism.

f) **CAP** stands for Customer Acceptance Policy as stated in this Policy.

g) **RBI** stands for Reserve Bank of India.

h) **CIP** Stands for Customer Identification Procedure as stated in this policy.

i) **CDD** stands for Customer Due Diligence Procedure as stated in this policy.

j) **UCIC** stands for Unique Customer Identification Code.

k) **CKYCR** stands for Central KYC Records Registry.

l) **V-CIP** stands for Video-based Customer Identification Process.

m) **EDD** means Enhanced Due Diligence

n) **OVD** means officially valid documents as defined under the RBI KYC Directions from time to time

o) **PEP** means Politically Exposed Person.

p) **Beneficial Owner** shall have the meaning assigned under the RBI KYC Directions, 2025 and the Prevention of Money-laundering Rules.

q) **Principal Officer** means the officer designated by the Company under the Prevention of Money-laundering Act, 2002 for monitoring and reporting obligations.

r**) Designated Director** means the Director nominated by the Board under the Prevention of Money-laundering Act, 2002 and Rules made thereunder.

s) **Senior Management** means one or more officers of the Company authorised by the Board of Directors to exercise powers or perform functions under this Policy.

Any term not defined in this Policy shall have the meaning assigned to it under the Prevention of Money-laundering Act, 2002, the Rules made thereunder, the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025 or any other applicable law.

3. Objectives, Scope and Application of the Policy:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help to manage its risks prudently. Thus, the KYC policy has been framed by the Company for the following purposes:

i. To prevent the Company from being used, intentionally or unintentionally, for money laundering, terrorist financing or other unlawful activities.

ii. To ensure compliance with the Prevention of Money-laundering Act, 2002, Prevention of Money-laundering (Maintenance of Records) Rules, 2005, RBI KYC Directions, 2025 and other applicable laws.

iii. To establish a robust Customer Acceptance Policy, Customer Identification Procedure and Customer Due Diligence framework.

iv. To identify, assess, monitor and mitigate Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks.

v. To ensure timely reporting of prescribed transactions to the Financial Intelligence Unit – India (FIU-IND).

vi. To ensure periodic updation of customer KYC records.

vii. To provide guidance to employees regarding KYC/AML/CFT compliance.

viii. To protect the Company from reputational, operational, legal and regulatory risks.

This Policy shall apply to all offices, branches, business locations, employees and officials of the Company and shall be read together with all internal operating procedures issued by the Company from time to time. This Policy comprises the following key elements:

I. Customer Acceptance Policy (CAP)
II. Customer Identification Procedures (CIP)
III. Customer Due Diligence Procedure (CDD procedure)
IV. Risk management
V. Training Program
VI. Internal Control Systems
VII. Record Keeping
VIII. Appointment of Principal Officer
IX. Reporting to Financial Intelligence Unit – India
X. General
XI. Compliance of KYC Policy
XII. Other Operating Instructions
XIII. Revision of Policy

4. Key elements:

I. Customer Acceptance policy (CAP)

The Customer Acceptance Policy lays down the principles for acceptance of customers and shall ensure that the Company does not knowingly establish or continue a business relationship with persons involved in Money Laundering, Terrorist Financing, Proliferation Financing or any other unlawful activity.

The Company shall adhere to the following principles:

a) No account or customer relationship shall be opened or established in an anonymous, fictitious or benami name.

b) Customer identity shall be verified in accordance with the Customer Identification Procedure (CIP) and Customer Due Diligence (CDD) requirements before establishing any business relationship or undertaking any transaction requiring CDD.

c) No transaction or business relationship shall be undertaken without carrying out the applicable Customer Due Diligence.

d) Where the Company is unable to apply appropriate Customer Due Diligence due to non-cooperation of the customer or unreliability of the information or documents furnished, the Company shall not establish or continue the business relationship and shall consider filing a Suspicious Transaction Report (STR), wherever applicable.

e) Mandatory KYC information shall be obtained at the commencement of the business relationship and during periodic KYC updation. Any additional information shall be obtained only with the explicit consent of the customer.

f) Customer Due Diligence shall be carried out for all holders in case of joint relationships.

g) The Company shall maintain a Unique Customer Identification Code (UCIC) for every customer in accordance with the RBI Directions.

h) The Company shall maintain customer KYC records and update the Central KYC Records Registry (CKYCR) in accordance with the applicable laws and RBI Directions.

i) Customers shall be classified into Low Risk, Medium Risk and High-Risk categories based on the Company's Risk Assessment Framework.

j) Accounts of Politically Exposed Persons (PEPs) and other High-Risk customers shall be dealt with in accordance with the Enhanced Due Diligence provisions of this Policy.

k) Implementation of this Policy shall not become unduly restrictive or result in denial of financial services to members of the general public, particularly financially or socially disadvantaged persons, including persons with disabilities.

l) Aadhaar shall not be insisted upon as a mandatory KYC document except where specifically permitted or required under applicable law.

m) As a matter of business policy, customers below 21 years of age shall not be eligible to avail loan facilities unless otherwise approved by the Board or under any specific product approved by the Company.

n) The Company shall not establish or continue a business relationship where the customer's identity cannot be satisfactorily established or where the Company suspects that the customer or transaction is connected with Money Laundering, Terrorist Financing, Proliferation Financing or any other unlawful activity.

o) The Company shall conduct sanctions screening and other necessary checks against applicable regulatory lists before establishing a customer relationship and thereafter on an ongoing basis.

II. Customer Identification Procedures ("CIP")

Customer Identification means identifying the customer and verifying the customer's identity by using reliable, independent source documents, data or information before establishing a business relationship or carrying out any transaction requiring Customer Due Diligence (CDD).

The Company shall obtain sufficient information to establish the identity of the customer, beneficial owner, authorised signatory and the person acting on behalf of the customer, wherever applicable.

The Company may undertake customer identification through Physical KYC, Digital KYC, Aadhaar Offline Verification, Aadhaar based e-KYC (where permitted), Video-based Customer Identification Process (V-CIP), Central KYC Records Registry (CKYCR) and equivalent e-documents in accordance with the RBI Directions.

Customer Identification shall be carried out in the following cases:

a) Before establishing any business relationship with a customer.

b) Before carrying out any transaction for a walk-in customer involving ₹50,000 or more, whether as a single transaction or a series of connected transactions.

c) Whenever there is doubt about the authenticity or adequacy of the customer's identification documents or information.

d) Whenever the Company suspects that the customer is intentionally structuring transactions below the prescribed threshold to avoid reporting requirements.

e) Before undertaking international money transfer transactions, wherever applicable.

f) Before selling third-party financial products or undertaking any activity requiring customer identification under the applicable RBI Directions.

The Company shall satisfy itself regarding the genuineness of the customer's identity and shall not rely merely on collection of documents.

The Company shall not insist upon any introduction for establishing a customer relationship.

III: Customer Due Diligence Procedure (CDD)

Customer Due Diligence (CDD) shall be carried out before establishing a business relationship and thereafter on an ongoing basis in accordance with the RBI Directions.

A. Customer Due Diligence for Individuals

Before establishing a business relationship with an individual customer, the Company shall obtain:

a) Officially Valid Documents (OVDs) as specified in Annexure–1 for proof of identity and address.

b) One recent live photograph captured through the Company's approved KYC system.

c) Permanent Account Number (PAN) or Form No.60, wherever applicable.

d) KYC Identifier, wherever available, with the customer's consent for downloading records from CKYCR.

e) Information relating to occupation, nature of business, source of income, source of funds, financial status and such other information as may be necessary based on the customer's risk profile.

Where a customer voluntarily submits Aadhaar or opts for Aadhaar Offline Verification, the Company shall comply with the Aadhaar Act, 2016 and the applicable RBI Directions.

Where Aadhaar details are collected, the Aadhaar Number shall be masked or redacted wherever required.

The Company may use Digital KYC, Aadhaar Offline Verification, equivalent e-documents and V-CIP in accordance with the RBI Directions.

B. Customer Due Diligence through Third Party

The Company may rely upon Customer Due Diligence carried out by another Regulated Entity, subject to the following conditions:

a) Customer Due Diligence records shall be obtained from the third party or through CKYCR within two days.

b) Copies of customer identification documents and other relevant records shall be made available immediately whenever requested.

c) The third party shall be regulated, supervised and monitored for compliance with the Prevention of Money-laundering Act, 2002 and applicable regulatory requirements.

d) The third party shall not be located in a country or jurisdiction identified by the Financial Action Task Force (FATF) as having inadequate AML/CFT measures.

Notwithstanding such reliance, the ultimate responsibility for Customer Due Diligence shall always remain with AFPL.(The description of Regulated Entities is provided in **Annexure – 2**.)

C. Selling third party products

Wherever the Company undertakes distribution of third-party financial products, it shall ensure that:

a) Customer Identification Procedure (CIP) and Customer Due Diligence (CDD) are completed before undertaking the transaction.

b) Officially Valid Documents (OVDs), PAN or Form No.60 and such other documents as required under applicable laws are obtained and verified.

c) The identity of the beneficial owner, authorised signatory or person acting on behalf of the customer is verified, wherever applicable.

d) Customer records relating to third-party products are maintained in accordance with this Policy.

e) Transactions relating to third-party products are monitored under the Company's AML monitoring framework and suspicious transactions, wherever identified, are reported in accordance with the Prevention of Money-laundering Act, 2002 and RBI Directions.

D. Monitoring of Transactions

The Company shall continuously monitor customer transactions throughout the business relationship and adopt a Risk-Based Approach to identify unusual or suspicious transactions.

Special attention shall be given to:

i. Complex transactions.

ii. Unusually large transactions.

iii. Transactions having no apparent economic or lawful purpose.

iv. Transactions involving high-risk jurisdictions.

v. Transactions inconsistent with the customer's profile, occupation, source of income or expected transaction behaviour.

vi. Transactions suspected to involve Money Laundering (ML), Terrorist Financing (TF) or Proliferation Financing (PF).

Illustrative examples of suspicious transactions are provided in Annexure–3.

Where a transaction is found to be suspicious, the Company shall examine the transaction immediately and the Principal Officer shall file a Suspicious Transaction Report (STR) with FIU-IND as soon as possible, but not later than seven working days after arriving at the conclusion that the transaction is suspicious.

The Company shall also file the following reports with FIU-IND, wherever applicable:

a) Cash Transaction Report (CTR): All cash transactions exceeding ₹10 lakh and all connected cash transactions which together exceed ₹10 lakh during a month shall be reported on or before the 15th day of the succeeding month.

b) Counterfeit Currency Report (CCR): All transactions involving forged or counterfeit currency notes or bank notes shall be reported on or before the 15th day of the succeeding month.

c) Non-Profit Organisation Transaction Report (NTR): All reportable transactions involving receipts by Non-Profit Organisations (NPOs) of ₹10 lakh or more shall be reported on or before the 15th day of the succeeding month.

d) Such other reports as may be prescribed under the Prevention of Money-laundering Act, 2002, the Rules made thereunder, RBI Directions or by FIU-IND shall be submitted within the prescribed timelines.

E. Ongoing Due Diligence

The Company shall undertake ongoing due diligence throughout the business relationship to ensure that transactions are consistent with:

i. Customer profile;

ii. Nature of occupation or business;

iii. Source of income and source of funds;

iv. Source of wealth, wherever applicable;

v. Nature of the business relationship; and

vi. Customer's risk category.

High-Risk customers shall be subjected to Enhanced Due Diligence and closer monitoring.

The Company shall review the customer's risk categorisation periodically and whenever there is a material change in the customer's profile, business, transaction behaviour or risk perception.

F. Periodic Updation

Periodic KYC updation shall be carried out as follows:

i. High-Risk Customers – at least once every two years.

ii. Medium-Risk Customers – at least once every eight years.

iii. Low-Risk Customers – at least once every ten years,

or at such intervals as may be prescribed by the Reserve Bank of India from time to time.

During periodic KYC updation:

a) Customer Due Diligence records shall be updated.

b) Fresh KYC documents shall be obtained, wherever required.

c) Changes in name, address, occupation, mobile number, e-mail address and other KYC information shall be updated.

d) Customers may submit Officially Valid Documents through physical or digital mode, wherever permitted.

e) AFPL shall issue at least three advance reminders before the due date for periodic KYC updation (for example, 90 days, 60 days and 30 days before the due date), including at least one reminder by letter, wherever applicable. AFPL shall maintain records of all such communications and, wherever possible, use the customer's KYC details available in CKYCR to facilitate easier KYC updation.

f) Where the customer fails to complete periodic KYC updation, AFPL shall issue at least three additional reminders, informing the customer of the procedure for updation, consequences of non-compliance and the available escalation mechanism.

g) An acknowledgement shall be issued upon successful completion of KYC updation.

h) Customers may complete periodic KYC updation through any branch or through any other channel permitted by the RBI.

Note: The above timelines shall be reckoned from the date of commencement of the business relationship or the date of the last successful KYC updation, as applicable.

G. Enhanced Due Diligence

Enhanced Due Diligence shall be applied to High-Risk customers and such other customers as may be identified by the Company based on its Risk Assessment Framework or regulatory requirements.

Enhanced Due Diligence may include:

a) Obtaining additional identity and address documents.

b) Obtaining information relating to source of income, source of funds and source of wealth.

c) Obtaining information regarding occupation, business activities and expected transaction pattern.

d) Obtaining approval from Senior Management before establishing or continuing the business relationship, wherever required.

e) Enhanced monitoring of transactions.

f) More frequent review and updation of KYC records.

H. Politically Exposed Persons (PEPs)

Relationships with Politically Exposed Persons shall be established only after approval of Senior Management.

The Company shall:

i. establish the source of wealth and source of funds;
ii. conduct enhanced due diligence;
iii. undertake continuous monitoring of transactions; and
iv. continue enhanced monitoring even after the customer ceases to be a PEP until the associated risk is considered to have reduced.

I. High Net worth Individuals:

Special care and enhanced due diligence shall be exercised while establishing or continuing business relationships with High Net Worth Individuals (HNIs). Such relationships shall be subject to enhanced monitoring based on the Company's Risk Assessment Framework.

IV. Risk Management

The Company shall adopt a Risk-Based Approach (RBA) for identifying, assessing, monitoring and mitigating Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks.

A. Customer Risk Categorisation

Every customer shall be classified into one of the following categories based on the Company's Board-approved Risk Assessment Framework:

i. High Risk

ii. Medium Risk

iii. Low Risk

The risk categorisation shall be based on one or more of the following factors:

a) Nature of customer.

b) Occupation or business.

c) Financial status.

d) Source of income and source of funds.

e) Source of wealth, wherever applicable.

f) Geographical location.

g) Delivery channels.

h) Products and services availed.

i) Transaction pattern and expected account activity.

j) Politically Exposed Person (PEP) status.

k) Adverse media reports.

l) Sanctions screening results.

m) Countries or jurisdictions identified by FATF.

n) Any other ML/TF/PF risk identified by the Company.

The risk categorisation shall be reviewed periodically and whenever there is a material change in the customer's profile, business activities, ownership, transaction pattern or any other relevant information.

B. Enterprise-wide Risk Assessment

The Company shall conduct an Enterprise-wide Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF) Risk Assessment at least once every year or earlier whenever there are material changes in:

a) Products or services;

b) Customer base;

c) Delivery channels;

d) Geographical exposure;

e) Technology;

f) Business model; or

g) Applicable regulatory requirements.

The findings of the Risk Assessment shall be documented and used for strengthening the Company's internal controls, customer due diligence measures and transaction monitoring framework.

V. Training Program

AFPL shall have an ongoing employee training programs so that the staffs are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/ staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

VI. Internal Control System

The Company shall establish an effective Internal Control System to ensure proper implementation of this Policy.

The Internal Control System shall include:

a) Independent compliance monitoring.

b) Periodic Internal Audit.

c) Monitoring of KYC compliance.

d) Identification of deficiencies.

e) Corrective and preventive actions.

f) Reporting to the Board of Directors.

The Board of Directors shall ensure that:

i. adequate systems and procedures are established for KYC compliance;

ii. sufficient resources are made available;

iii. deficiencies observed during audits are rectified promptly;

iv. compliance reports are placed before the Board at periodic intervals.

The Company shall establish appropriate employee screening procedures at the time of recruitment to minimise the risk of employing persons having criminal background or doubtful integrity.

The Internal Audit function shall independently review compliance with this Policy, the RBI Directions and the Prevention of Money-laundering Act and submit its observations together

with corrective action taken reports to the Board of Directors or the Audit Committee, as applicable.

VII. Record Keeping

The Company shall maintain records in accordance with Section 12 of the Prevention of Money-laundering Act, 2002, the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 and the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025.

The Company shall:

a) maintain records of all domestic and international transactions for at least five years from the date of the transaction;

b) preserve customer identification records and KYC documents for at least five years after the end of the business relationship;

c) make identification records and transaction details available to competent authorities whenever required.

The Company shall maintain records of the following transactions:

i. Cash transactions exceeding ₹10 lakh or its equivalent in foreign currency.

ii. Series of cash transactions which are individually below ₹10 lakh but are connected and together exceed ₹10 lakh during a month.

iii. Transactions involving receipts by Non-Profit Organisations (NPOs) of ₹10 lakh or more.

iv. Transactions involving forged or counterfeit currency notes or bank notes.

v. Suspicious transactions, whether or not made in cash.

For every reportable transaction, the Company shall maintain records of:

a) Nature of transaction.

b) Amount involved.

c) Currency.

d) Date of transaction.

e) Parties to the transaction.

The Company shall establish an appropriate system for maintenance, preservation and retrieval of records so that the required information can be produced promptly whenever called for by the Reserve Bank of India, Financial Intelligence Unit – India (FIU-IND) or any other competent authority.

VIII. Appointment of Principal Officer

The Board of Directors shall designate the Company Secretary of the Company as the Principal Officer under the Prevention of Money-laundering Act, 2002 and the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025. In the event the position of Company Secretary is vacant or the Board considers it appropriate, the Board may designate any other senior management officer as the Principal Officer until a Company Secretary is appointed or a fresh designation is made by the Board..

Duties of the Principal Officer

The Principal Officer shall be responsible for:

a) Monitoring the implementation of this Policy.

b) Ensuring compliance with the Prevention of Money-laundering Act, 2002, the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 and the RBI KYC Directions.

c) Monitoring and examining suspicious transactions.

d) Filing Suspicious Transaction Reports (STR), Cash Transaction Reports (CTR) and other prescribed reports with FIU-IND within the prescribed timelines.

e) Acting as the nodal officer for coordination with FIU-IND, RBI and other competent authorities.

f) Ensuring timely submission of all regulatory reports and information.

g) Maintaining confidentiality of reports and information furnished under the PMLA.

h) Reporting significant KYC/AML/CFT compliance issues to the Board of Directors and Senior Management.

The Company shall intimate the appointment and any subsequent change in the Principal Officer to FIU-IND, RBI and such other authorities, wherever required under the applicable laws.

IX. Reporting to Financial Intelligence Unit – India

The Principal Officer shall ensure timely submission of all reports required under the Prevention of Money-laundering Act, 2002, the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 and the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025.

The Company shall report, wherever applicable:

a) Suspicious Transaction Reports (STR);

b) Cash Transaction Reports (CTR);

c) Counterfeit Currency Reports (CCR);

d) Non-Profit Organisation Transaction Reports (NTR); and

e) Any other report prescribed under the applicable laws.

All reports shall be submitted through the reporting mechanism prescribed by FIU-IND within the prescribed timelines.

The Company, its Directors, officers and employees shall maintain strict confidentiality regarding the reporting of suspicious transactions and shall not disclose to the customer or any other person that a report has been filed or is proposed to be filed with FIU-IND, except as permitted under applicable law.

X. General

A. Central KYC Records Registry (CKYCR)

The Company shall capture and upload the KYC records of customers to the Central KYC Records Registry (CKYCR) in accordance with the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 and the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025.

The Company shall:

i. Upload the customer's KYC records to the Central KYC Records Registry (CKYCR) within 10 days from the commencement of the business relationship with the customer

ii. communicate the KYC Identifier generated by CKYCR to the customer;

iii. update customer KYC records in CKYCR whenever required under the applicable laws and RBI Directions; and

iv. use CKYCR records, wherever available and permitted, to facilitate Customer Due Diligence and periodic KYC updation.

B. Introduction of New Technologies

The Company shall pay special attention to Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks that may arise from new or developing technologies, products, services and delivery channels, including digital and online transactions that may favour anonymity.

Before introducing any new product, service, technology or delivery channel, the Company shall:

i. identify and assess the associated ML/TF/PF risks;

ii. implement appropriate risk mitigation measures;

iii. establish suitable internal controls; and

iv. ensure ongoing monitoring of such risks

C. Closure of Business Relationship

Where the Company is unable to apply appropriate Customer Due Diligence measures due to:

i. non-furnishing of information;

ii. non-cooperation by the customer;

iii. failure to complete KYC requirements; or

iv. unreliability of the documents or information furnished,

the Company may decline to establish or continue the business relationship after giving due notice to the customer, wherever applicable.

Such decision shall be taken by the authority authorised by the Board of Directors.

Wherever required, the Company shall also consider filing a Suspicious Transaction Report (STR) with the Financial Intelligence Unit – India (FIU-IND).

D. Existing Customers

The Company shall ensure that all existing customers comply with the applicable KYC requirements prescribed under the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025.

Wherever PAN or Form No.60 is required under applicable law, the Company shall obtain the same within the prescribed timelines.

Where a customer fails to furnish PAN or Form No.60, the Company shall take appropriate action in accordance with the applicable statutory provisions after giving reasonable notice and an opportunity to comply.

In deserving cases, such as injury, infirmity, old age or any other genuine reason, the Company may permit appropriate relaxation for submission of documents for a maximum period of six months, subject to:

i. approval of Senior Management; and

ii. compliance with the applicable RBI Directions and other laws.

Existing customer relationships shall continue to be monitored on an ongoing basis and shall be subjected to periodic KYC updation in accordance with this Policy.

E. Updating of KYC Policy

The Principal Officer shall continuously monitor amendments to:

i. the Prevention of Money-laundering Act, 2002;

ii. the Prevention of Money-laundering (Maintenance of Records) Rules, 2005;

iii. the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025; and

iv. other applicable laws and regulatory guidelines.

Wherever necessary, the Principal Officer shall recommend suitable amendments to this Policy.

Any amendment or modification to this Policy shall become effective only after approval by the Board of Directors.

F. Unique Customer Identification Code (UCIC)

The Company shall allot a Unique Customer Identification Code (UCIC) to every customer in accordance with the RBI Directions.

The UCIC shall be used to:

i. uniquely identify every customer across all business relationships;

ii. facilitate Customer Due Diligence;

iii. enable effective transaction monitoring;

iv. strengthen risk management; and

v. comply with regulatory reporting requirements.

XI. Compliance of KYC Policy

The Company shall establish an effective compliance framework to ensure implementation of this Policy.

Accordingly:

a) The Internal Audit and Compliance functions shall periodically review compliance with this Policy and the applicable statutory and regulatory requirements.

b) Compliance reports together with deficiencies observed and corrective action taken shall be placed before the Board of Directors.

c) Any non-compliance with this Policy shall be viewed seriously and appropriate corrective or disciplinary action shall be initiated wherever necessary.

d) The Company shall ensure that deficiencies identified during inspections, internal audits, statutory audits or regulatory examinations are rectified within the prescribed timelines.

XII. Other Operating Instructions

a) Where no transaction has been carried out by a customer for a continuous period of twelve months, the Company may review the customer's KYC records and obtain updated KYC documents, wherever required, based on the customer's risk profile and the applicable RBI Directions.

b) As a matter of business policy, the Company shall grant Gold Loans only to individual borrowers and not to companies, partnership firms, limited liability partnerships, trusts or other non-individual entities unless otherwise approved by the Board of Directors.

c) The Company shall ensure that KYC procedures are implemented in a fair, dignified and non-discriminatory manner for all customers, including pardanashin women, senior citizens, persons with disabilities and other vulnerable customers, while ensuring that their identity is satisfactorily established and documented in accordance with the applicable laws and the RBI Directions.

d) Customer information obtained under this Policy shall be kept confidential and shall be used only for lawful purposes connected with Customer Due Diligence, regulatory reporting, risk management and compliance with applicable laws.

e) The Company shall ensure that all employees maintain confidentiality of customer information and shall not disclose such information except where disclosure is permitted or required under law

XIII. Revision of Policy

This Policy shall be reviewed by the Board of Directors:

at least once every year; or earlier, whenever required due to amendments in:

i. the RBI (Non-Banking Financial Company – Know Your Customer) Directions, 2025;

ii. the Prevention of Money-laundering Act, 2002;

iii. the Prevention of Money-laundering (Maintenance of Records) Rules, 2005; or

iv. any other applicable law or regulatory guideline.

All amendments approved by the Board shall form part of this Policy from the effective date approved by the Board.

Annexure-1

Officially Valid Documents (OVD)

Officially Valid Document (OVD) means any one of the following documents:

1. Individuals

i. Passport;

ii. Driving Licence;

iii. Proof of possession of Aadhaar Number in such form as issued by the Unique Identification Authority of India (UIDAI), where submitted in accordance with the applicable laws and RBI Directions;

iv. Voter's Identity Card issued by the Election Commission of India;

v. Job Card issued by NREGA duly signed by an officer of the State Government;

vi. Letter issued by the National Population Register containing the details of name and address.

Provided that:

a) Where the customer submits proof of possession of Aadhaar Number as an OVD, it shall be accepted only in such form as issued by UIDAI.

Note: Aadhaar shall not be mandatory for KYC except where required under applicable law or where voluntarily submitted by the customer in accordance with the RBI Directions.

b) Where the OVD furnished by the customer does not contain the current address, the following documents or equivalent e-documents shall be accepted as proof of address for the limited purpose of establishing the current address:

i. Utility bill (electricity, telephone, post-paid mobile phone, piped gas or water bill) not more than two months old;

ii. Property or Municipal Tax Receipt;

iii. Pension or Family Pension Payment Order (PPO);

iv. Letter of allotment of accommodation issued by Government Departments, statutory or regulatory bodies, Public Sector Undertakings, scheduled commercial banks, financial institutions or listed companies, and Leave and Licence Agreement executed with such employers.

c) The customer shall submit an OVD containing the current address within three months from the date of submission of the above documents.

d) Where the OVD submitted by a foreign national does not contain the address, documents issued by Government authorities of the foreign jurisdiction or a letter issued by the Foreign Embassy or Foreign Mission in India shall be accepted as proof of address.

Explanation: 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, Gazette Notification or any other document evidencing such change in accordance with applicable law.

2. Sole Proprietary Concern

In addition to the KYC documents of the proprietor, AFPL shall obtain any two of the following documents as proof of the existence of the business/activity:

i. Registration Certificate;

ii. Certificate or Licence issued by the Municipal Authorities under the Shop and Establishment Act;

iii. GST Registration Certificate;

iv. Certificate or Registration Document issued by any professional body governing the business;

v. Licence issued by the registering authority in the name of the proprietary concern;

vi. IEC (Importer Exporter Code) issued by the Directorate General of Foreign Trade;

vii. Complete Income Tax Return (not merely acknowledgement), where the business income is reflected;

viii. Utility bills in the name of the proprietary concern.

Where the above documents are not available, AFPL may accept such other documents as permitted under the RBI Directions after satisfying itself regarding the existence of the business.

3. Companies

AFPL shall obtain:

i. Certificate of Incorporation;

ii. Memorandum of Association;

iii. Articles of Association;

iv. Permanent Account Number (PAN) of the Company;

v. Board Resolution authorising the authorised signatory;

vi. Officially Valid Document of the authorised signatory;

vii. Proof of authority of the authorised signatory to act on behalf of the Company;

viii. Beneficial Ownership information, wherever applicable.

4. Partnership Firms

AFPL shall obtain:

i. Registration Certificate (if registered);

ii. Partnership Deed;

iii. PAN of the Partnership Firm;

iv. Officially Valid Document of the authorised partner(s);

v. Authority letter authorising the person acting on behalf of the firm;

vi. Beneficial Ownership information, wherever applicable.

Annexure-2

Regulated Entities:

a) All Scheduled Commercial Banks (SCBs), Regional Rural Banks (RRBs), Local Area Banks (LABs), Primary (Urban) Co-operative Banks (UCBs), State Co-operative Banks (StCBs), Central Co-operative Banks (CCBs) and any other banking company or banking institution licensed under Section 22 of the Banking Regulation Act, 1949.

b) All India Financial Institutions (AIFIs).

c) All Non-Banking Financial Companies (NBFCs), including such categories of NBFCs as may be regulated by the Reserve Bank of India from time to time.

d) All Payment System Providers (PSPs), System Participants (SPs) and Prepaid Payment Instrument (PPI) Issuers authorised by the Reserve Bank of India.

e) All Authorised Persons (APs), including entities acting as agents under the Money Transfer Service Scheme (MTSS), authorised by the Reserve Bank of India.

f) Depository Participants (DPs) registered with the Securities and Exchange Board of India (SEBI).

Annexure-3

Illustrative List Of Suspicious Transactions

The following is an illustrative list of suspicious transactions and activities that may indicate possible money laundering, terrorist financing or other unlawful activities. The list is not exhaustive, and AFPL shall examine any transaction that appears unusual or gives rise to reasonable suspicion, based on the facts and circumstances of each case.

1. Identity of Customer

a) Submission of forged, counterfeit, altered or false identification documents.

b) Identification documents or information that cannot be verified within a reasonable time.

c) Use of fictitious, benami or misleading names.

d) Multiple customers using the same identity, address, mobile number, e-mail address or other identifying particulars without any apparent legitimate reason.

e) Attempts to conceal the identity of the beneficial owner or the person on whose behalf the customer is acting.

2. Background of Customer

a) Customer having known or suspected links with criminals, terrorist organisations or persons involved in money laundering or other unlawful activities.

b) Adverse media reports or other credible information indicating possible involvement in fraud, financial crimes or other illegal activities.

c) Customer unwilling to disclose the nature of business, source of funds or source of wealth without reasonable justification.

3. Multiple Customer Relationships

a) Large number of customer relationships having a common customer, authorised representative, address, mobile number, e-mail address or other common identifiers without any apparent legitimate purpose.

b) Multiple customer relationships maintained without any reasonable explanation.

c) Frequent opening and closure of customer relationships without any apparent business purpose.

4. Transactions without Apparent Rationale

a) Unexplained transfers or movement of funds with no apparent economic or lawful purpose.

b) Transactions routed through third-party accounts without satisfactory explanation.

c) Requests for payments or loan disbursements to unrelated third parties without any apparent legitimate reason.

5. Activity in Customer Relationship

a) Sudden or unusual activity in dormant or inactive customer relationships.

b) Transactions inconsistent with the customer's declared occupation, business, income, financial position or expected transaction profile.

c) Significant increase in transaction volume without any apparent legitimate reason.

d) Frequent changes in address, mobile number, e-mail address or other KYC information without reasonable explanation.

6. Nature of Transactions

a) Unusually complex transactions.

b) Transactions having no apparent economic or lawful purpose.

c) Frequent transactions inconsistent with the customer's profile, business or financial standing.

d) Transactions involving high-risk jurisdictions or persons subject to sanctions, where applicable.

e) Structuring or splitting of transactions to avoid regulatory reporting or Customer Due Diligence requirements.

7. Value of Transactions

a) Transactions just below the prescribed reporting threshold, indicating an apparent attempt to avoid reporting requirements.

b) Transactions inconsistent with the customer's known financial position or source of funds.

c) Large or unusual transactions without satisfactory explanation.

8. Other Indicators of Suspicious Transactions

a) Customer is reluctant to provide information, documents or explanations required for Customer Due Diligence.

b) Submission of forged, fabricated or misleading documents or information.

c) Reluctance or refusal to disclose the source of funds or source of wealth, where required.

d) Repeated attempts to avoid Customer Due Diligence or identity verification procedures.

e) Use of intermediaries, representatives or third parties without any apparent legitimate reason.

f) Attempts to improperly influence or circumvent AFPL's credit appraisal, KYC or internal control procedures.

g) Doubt regarding the identity of the beneficial owner.

h) Loan proceeds being credited to or routed through accounts not belonging to the customer without satisfactory explanation.

i) Utilisation of loan proceeds for purposes materially different from those declared at the time of sanction.

j) Frequent requests for changes in customer information without reasonable explanation.

k) Overpayment of loan instalments followed by requests for refund of the excess amount.

l) Transactions involving persons or entities appearing in sanctions lists or other lists issued by competent authorities.

m) Any transaction or attempted transaction which, in the opinion of AFPL, appears unusual, lacks an apparent economic or lawful purpose, or gives rise to a reasonable ground to suspect money laundering, terrorist financing or proliferation financing.

****