CIN : U65999UP2017PTC089516

ARYADHAN FINANCIAL SOLUTIONS PRIVATE LIMITED

KYC & AML POLICY

Release Date	11th November, 2025
Version No.	1.1
Policy Owner	Credit-Product Department & Compliance Department
Approved By	Board of Directors

Aryadhan Financial Solutions Pvt. Ltd.
H-82, First Floor, Sector-63, Noida,
Uttar Pradesh-201301

91-120-4859300
info@aryadhan.co.in
www.aryadhan.co.in

INTRODUCTION

Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC)norms and Anti-money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

This Policy requires the Company and each Employee to:

- Protect the Company from being used for money laundering or funding terrorist activities
- Comply with the letter and the spirit of applicable AML/CTF Laws, and the Company's AML Program and procedures
- Be alert to and escalate suspicious activity
- Cooperate with AML-related law enforcement and regulatory agencies to the extent permitted under applicable laws.

Accordingly, in compliance with the guidelines issued by **RBI- Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time**, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company. This policy is applicable to all categories of products and services offered by the Company.

OBJECTIVE

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionallyby criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

KEY ELEMENTS OF POLICY

The Company is hereunder framing its KYC Policy incorporating the following four key elements:

- Customer Acceptance Policy (CAP)
- Risk management
- Customer Identification Procedures (CIP)
- Monitoring of Transactions

CUSTOMER ACCEPTANCE POLICY

The Company shall follow the following norms while accepting and dealing with its customers:

Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his/her clients, mode of payments, volume of turnover, social and

financial status etc. to enable categorization of customers into low, medium and high risk.

The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his/her clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive.

A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers. CDD procedure shall be conducted at the UCIC level. Thus, if an existing KYC compliant customer desires to open another account or avail any other product or service, conducting fresh CDD exercise as far as identification of the customer is concerned not mandatory.

The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged including the Persons with Disabilities (PwDs). While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers. No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the Credit Department.

The Company shall carry out full scale customer due diligence (CDD) before opening an account. If an existing KYC compliant customer desires to open another account or avail any other product or service from Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned. When the true identity of the account holder is not known, the Company shall file Suspicious Transaction Reporting (STR). The Company shall not pursue the customer due diligence (CDD) if it is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the customer due diligence (CDD) process will tip-off the customer and instead the company shall file an Suspicious Transaction Reporting (STR).

The Company shall ensure that the identity of the customer does not match with any person or entity whose name appears in the sanction lists / designated lists circulated by RBI from time to time.

The company shall ensure that:

a) No account is opened in fictitious / benami name or where the company is unable to do customer due diligence either on account of non-cooperation of the customer or non-reliability of the documents/ information given by customer
b) System is in place to check the identify of customer doesn't match with any person / entity, whose name appears in the sanctions of RBI.
c) Filing an STR is considered, if necessary when it is unable to comply with the relevant CDD measures in relation to the customer.
d) Additional information, where such information requirement has not been specified in the internal KYC Policy of the Company, is obtained with the explicit consent of the customer.

CUSTOMER IDENTIFICATION PROCEDURE

Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious person. The Customer Identification Procedure (CIP) to be carried out at different stages i.e. while establishing a business relationship; creating an account based relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.

An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 ("Act") and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

- Verify the identity of any Person transacting with the Company to the extent reasonable and practicable
- Maintain records of the information used to verify a customer's identity, including name, address and other identifying information and
- Consult lists of known or suspected terrorists or terrorist organizations provided to the Company by any applicable government agency to determine whether a person opening an account or an existing customer appears on any such list.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

The Company will carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc. The internal risk assessment carried out by the Company should commensurate to its size, geographical presence, complexity of activities/structure, etc. and shall apply a Risk Based Approach and implement a CDD programme, having regard to the ML/TF risks identified for mitigation and management of the identified risks. Respective businesses shall have standard operating procedures for identification, mitigation, controls and procedures for management of the identified risk, if any. The risk assessment processes shall be reviewed periodically to ensure its robustness and effectiveness.

REQUIRED KYC DUE DILIGENCE FOR ALL CUSTOMERS

Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. The Company shall take reasonable measures to ascertain and verify the true identity of allcustomers who transact with the Company.:

Type of documents
Documents to be collected from the applicant / co-applicant / guarantor / any other party to the loan are as follows:

KYC and other documents -
- Application form with live photograph/ official stamp in case of legal entity
- Officially Valid Document ("OVD")
- Signature verification (Individual)
- Any other document as specified / defined in the Product Program for various individual/ non-individual entities from time to time.

Entity specific documents for Proprietor / Partnership / HUF/ Club/Trust / Societies / Unincorporated association or a body of individuals/ Limited Companies are:
- Proof of legal existence
- Proof of operating address
- Proof of registered address if different than operating address
- Signature verification of the authorised signatory of the entity

Refer **Annexure II** for the list of documents and manner of verification.

Modes of undertaking CDD:
Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:
a. the Aadhaar number where the individual decides to submit his Aadhaar number voluntarily under first proviso to sub-section (1) of section 11A of the PML Act. In such instances, Company shall carry out authentication of the individual's Aadhaar number using e-KYC authentication facility including Aadhaar Face Authentication provided by the UIDAI. Further, in such a case, if the individual wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he / she may submit a self declaration to that effect; or
b. the proof of possession of Aadhaar number where offline verification can be carried out; Company shall carry out offline verification of Aadhar. If offline verification cannot be carried out, the customer shall submit any other OVD or the equivalent e-document thereof containing the details of his identity and address carry out verification through digital KYC as prescribed under the RBI Directions or
c. where equivalent e-document of any OVD is obtained, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo or

d. the KYC Identifier with an explicit consent to download records from CKYCR; and
e. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Incometax Rules, 1962; and
f. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required.
g. V-CIP process as prescribed under the KYC Master Directions from time to time, may also be carried out as part of customer identification process, if deemed appropriate.

VERIFICATION

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable beliefthat it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

Verification through Documents:

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company. These are appropriately covered in the credit policies of the respective businesses. The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as Annexure I to this policy. These should be appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

Verification through non-documentary methods:

These methods may include, but are not limited to:

- Contacting or visiting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

Additional verification procedures:

If applicable, the business process verification procedures should address situationswhere:

- A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
- The business process associate is not familiar with the documents presented;
- The Account is opened without obtaining documents;

- Where the business process is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customerthrough documents; and
- If the business process cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

Where a low-risk category customer expresses inability to complete the documentation requirements on account of any reason that the Company considers tobe genuine, and where it is essential not to interrupt the normal conduct of business, the Company may complete the verification of identity within a period of six months from the date of establishment of the relationship.

RESOLUTION OF DISCREPENCIES

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

REPORTING

The Company shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs.10 lakhs, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a 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; 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 ofthe activities relating to terrorism.
e) Where the transactions are abandoned by customers on being asked to give some details or to provide documents

Further, the Compliance officer shall furnish information of the above-mentioned transactions to the Head Risk & Credit of the company at the prescribed address inthe formats prescribed in this regard including the electronic filing of reports.

Provided that where the Head Risk & Credit, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.10

lakhs so as to defeat the provisions of the PMLA regulations, shall furnish information in respect of such transactions to the Director within the prescribed time.

REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA: All transactions of cash and suspicious as required under PML Act 2002 shall be reported to Financial Intelligence Unit (FIU) from time to time. The Principal Officer shall ensure that such reporting system is in place and shall monitor receipt of the reports.

RECORD RETENTION

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

A) Transactions for which records need to be maintained:

1. All cash transactions of the value of more than Rs.10 lakhs or its equivalentin foreign currency.
2. All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a monthand the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.
3. All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency.
4. All cash transactions where forged or counterfeit currency notes orbank notes have been used as genuine and where any forgery of a valuable security has taken place.
5. All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.

B) Information to be preserved:

The information required to be preserved with respect to the above transactions are the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

C) Periodicity of retention:

The following records shall be retained for a minimum period of five years after the related account is closed:

1. The customer identification information and residence identification information including the documentary evidence thereof
2. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained for a period of at least five (5) years after such record was created.

The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

ENHANCED DUE DILIGENCE

The Company is primarily engaged in retail finance. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The existing credit policies of the Company in respect of its various businesses ensure that the Company is not transacting with such high-risk customers. The Company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. Each business processshall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence.

Enhanced Due Diligence shall be coordinated and performed by the Company, that may engage appropriate outside investigative services or consult appropriate vendor sold databases when necessary. Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

- Customers requesting for frequent change of address/contact details
- Sudden change in the loan account activity of the customers
- Frequent closure and opening of loan accounts by the customers
- Accounts of Politically Exposed Persons (PEP)

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorisation of risk, updation of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses

EDD in case of Non-face-to-face customer onboarding:

Non-face-to-face onboarding would include customer onboarding without meeting the customer physically or through V-CIP. Non-face-to-face would include use of digital channels such as CKYCR, DigiLocker, equivalent edocument, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs, where there is no physical interaction with the customer. Following EDD measures shall be undertaken for non-face-to-face customer onboarding.

i. V-CIP shall be provided as the first option to the customer for remote onboarding.
ii. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
iii. Apart from obtaining the current address proof, Company shall verify the current address through positive confirmation such as address verification letter, contact point verification, deliverables, etc. before disbursement of the loan.
iv. PAN shall be mandatory in such cases and it shall be verified from the verification facility of the issuing authority.
v. Company shall ensure that the first payment is effected through the customer's KYC-complied account.
vi. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to face manner or through V-CIP.

Accounts of Politically Exposed Persons (PEPs):

Politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the information available about the person in the public domain. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the contracts of the family members or close relatives of PEPs.

In a scenario wherein an account has to be opened for a PEP after a detailed assessment of the source of funds, identity of the PEP, Details on his activities carried out by him and his family members; it shall be approved by CRO / CCO, HD – Operations and MD/CEO prior to opening of an account. If an existing customer subsequently becomes a PEP, then approvals has to be taken from the above mentioned designated individuals in order to continue the relationship. Such account would be tagged as "High Risk Customers" and all the process and procedures, not limited to CDD measures, including enhanced monitoring would be applicable.

RELIANCE ON THIRD PARTY DUE DILIGENCE

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, the Company may rely on a third party;subject to the conditions that

- the Company immediately obtains necessary information of such client due diligence carried out by the third party;
- the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- the Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record- keeping requirements in line with the requirements and obligations under the Act;
- the third party is not based in a country or jurisdiction assessed as high risk; and
- the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

RISK CATEGORIZATION

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higherrisk perception on a customer. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.

The Company shall have a system in place for periodical updation of customer identification data after the account is opened. Full KYC exercise will be done at a periodicity not less than once in ten years in case of low-risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high-risk category customers. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC. Documents as specified will be taken/reviewed at the time of periodic updation.

Low risk category customers need not submit fresh proofs of identity and address at the time of periodic updation, in case of no change in status with respect to their identities and addresses and a self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such 'low risk' customers, they can forward a certified copy of proof of address by mail/post, etc. Fresh photographs will be obtained from minor customer on becoming major. Fresh CDD & KYC, if required may be carried out.

In case of Legal entities, if there is no change in KYC then a self-declaration will suffice but in case if change in KYC, the Company shall review the documents sought at the time of opening of account and obtain fresh certified copies through the registered email id of the legal entity.

All the customers under different product categories are categorized into low, medium and high

risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization. An indicative categorization for the guidance of businesses is provided in **Annexure – I**. Each business process adopts the risk categorization in their respective credit policies subject to confirmation by compliance based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. etc., Where businesses believe that a particular customer falling under a category mentioned below is inhis judgement falling in a different category, he may categorize the customer so, so long as appropriate justification is provided in the customer file. For completely secured retail finance products, such categorization may be waived.

UPDATION/ PERIODIC UPDATION OF KYC

RBI instructs the Regulated Entities (REs), including banks, that the customers' KYC Identifier shall be the first reference point for the purpose of establishing an account-based relationship or for verification of identity of customers. Accordingly, while onboarding customer, Company shall download customer's KYC records online from CKYCR with customer's consent without requiring him/ her to submit the same records again, unless there is a change in records available with CKYCR.
The processes of onboarding customer and updation/ periodic updation of KYC have been simplified and the same are given below:

A. Face-to-face mode for onboarding the customer

- Customer may be onboarded in face-to-face mode through Aadhaar biometric based e-KYC authenticating and, in such case, if customer wants to provide a current address, different from the address as per the identity information available in the UIDAI database (i.e., Central Identities Data Repository), he may give a self-declaration to that effect to the Company.
- Further, Digital KYC process is also allowed for customer onboarding.

B. Non-face-to-face (NFTF) modes for onboarding the customer

- Consent-based onboarding of customer in NFTF mode may be done using Aadhaar OTP based e-KYC authentication subject to certain conditions. Further, such account shall be placed under strict monitoring, and Customer Due Diligence (CDD) procedure shall be completed within a year.
- Customer onboarding in NFTF mode using digital modes such as KYC Identifier, equivalent e-documents, documents issued through DigiLocker, and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs are subject to certain conditions.

C. Customer onboarding using Video based Customer Identification Process (V-CIP)

- V-CIP is an alternate method of CDD by an authorised official of the RE by undertaking seamless, secure, live, informed and consent based audiovisual interaction with the customer to obtain identification information required for CDD purpose.

- V-CIP is treated on par with face-to-face onboarding.

D. Simplified process of updation and periodic updation of KYC

- Self-declarations - Company shall obtain self-declaration regarding "no change in KYC information" or "a change only in address details" from customers using digital and non-digital modes, through customer's email / mobile number registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of RE), letter, BCs, etc.
- The updation/ periodic updation of KYC records are allowed to be carried out at any office of the Company with which customer maintains the account.
- Aadhaar OTP based e-KYC and V-CIP are permitted for the purpose of updation/ periodic updation of KYC.
- Company have been directed to update customers' KYC information/ records based on the update notification received from CKYCR.

In respect of an individual customer who is categorized as low risk, Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. Company = shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

Due Notices for Periodic Updation of KYC

Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded in the Company's system against each customer for audit trail. The Company shall expeditiously implement the same but not later than January 01, 2026.

RISK MANAGEMENT

The Company has put in place appropriate procedures to ensure effective implementation ofKYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location geographical risk covering customers as well as transactions, type of products/services offered, delivery

channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive.

MONITORING OF TRANSACTIONS

As per Income Tax Act, 1961, Cash cannot be accepted by any person (Branch / collection staff) over and above Rs. 2,00,000/- (Two Lacs only) for a particular transaction or series of integrally connected transactions. The Company does not accept cash deposits in foreign currency.

As per Income Tax Act, 1961, for any Cash or its equivalent payment over and above Rs.10,000/- , a 'source of funds' declaration for such cash should be obtained from the Customer/person depositing / repaying the loan.

Note: Source of funds in cash is through 'sale of immovable property', then Cash or its equivalent for more than Rs. 20,000/- should not be accepted.

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactionsthat fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts have to be subjected to intensified monitoring.
The Company shall put in place an appropriate software application / mechanism to throwalerts when the transactions are inconsistent with risk categorization and updated profile of customers.

SECRECY OBLIGATION AND SHARING OF INFORMATION

The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the customer and itself. No details shall be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

CDD PROCERDURE AND SHARING OF KYC INFORMATION WITH CKYCR

Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, RBI KYC Direction issued from time to time, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. CERSAI guidelines for uploading will be applicable. The Company shall ensure that the KYC identifier is communicated to the individual/ LE as the case may be.

Whenever the RE obtains additional or updated information from any customer as per clause below in this paragraph or Rule 9(1C) of the PML Rules, Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC record of an existing customer, the RE shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the RE.

For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier if available from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

i. there is a change in the information of the customer as existing in the records of CKYCR; or
ii. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
iii. the validity period of downloaded documents has lapsed; or
iv. the RE considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

CUSTOMER EDUCATION AND EMPLOYEE TRAINING

The Company may prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joinees on the elements of KYC through various training programmes and e-mails.

APPLICABILITY TO BRANCHES AND SUBSIDARIES

The above guidelines shall also apply to the branches and subsidiaries of the Company in and outside India.

APPOINTMENT OF DESIGNATED DIRECTOR AND PRINCIPAL OFFICER

Mr. Chattanathan Devarajan, Managing Director of the Company, is the designated director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules. Mr. Inderjeet Singh, Chief Risk Officer, will be designated as Principal Officer who shall be responsible for furnishing of information.

Any change in details of the Principal Officer/ Designated Director shall be communicated to the Regulators within the timelines prescribed by them.

COMPLIANCE OF KYC POLICY

i. For the purpose of KYC compliance, the Managing Director, CEO, CRO, CFO, CCO and Head Operations are constituted as "Senior Management".
ii. For day to day operations Business Head and Head Operations would ensure that the KYC policies and procedures are implemented effectively and efficiently.
iii. The Internal Auditors, as appointed time to time by the company, would verify the adherence of the KYC policy during the normal course of conducting their auditing activities and would bring any deviation/discrepancy, if any, to the Audit Committee on quarterly intervals on a quarterly basis, the audit points.
iv. The decision-making function of the determining compliance with the KYC policy/norms will not be outsourced by the company.

REVIEW OF THE POLICY

This Policy may be amended, modified or supplemented from time to time to ensure compliance with any modification, amendment or supplementation to the Applicable Law or as may be otherwise prescribed by the Board from time to time.

In case of any amendment(s), clarification(s), circular(s) etc. issued by the relevant authorities, not being consistent with the provisions laid down under this Policy, then such amendment(s), clarification(s), circular(s) etc. shall prevail upon the provisions hereunder and this Policy shall stand amended accordingly from the effective date of such amendment(s), clarification(s), circular(s) etc.

<<Space left blank intentionally>>

Annexure I

Indicative list for Risk Categorisation

Low Risk Category

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk.

Illustrative examples are:

- Salaried employees whose salary structure is well-defined
- People belonging to lower economic strata of the society whose accounts show small balances and low turnover
- Government departments and Government-owned companies
- Statutory bodies & Regulators
- Farmers Producer Organisation (FPO)

Medium & High-Risk Category

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

Illustrative examples of medium risk category customers are:

a) Non-Resident customers
b) High Net worth Individuals with more than Rs. 5 crores.
c) Trust, charities, NGO's and Organization receiving donations
d) Companies having close family shareholding where ultimate beneficial ownership is not identifiable
e) Firms with 'sleeping partners'

Illustrative examples of high-risk category customers are:

1. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
2. Those with dubious reputation as per public information available

Annexure II

KYC Documents Matrix

Customer Type	Documents and KYC Requirements
Individuals (Primary Applicant)	- PAN Card (mandatory, verified electronically)
	- One Officially Valid Document (OVD): Aadhaar Card, Voter ID, Driving License, Passport, Utility Bill (not older than 3 months)
	- Recent address proof (if different from OVD address)
	- Recent passport-sized photograph and signature
	- Form 60 (if PAN not available)
	- Aadhaar e-KYC or Video KYC records for digital onboarding
Co-Applicant(s) / Joint Applicant(s)	- Same KYC documentation as Primary Applicant
	- PAN Card
	- One OVD and address proof
	- Photograph and signature
Proprietorship	- PAN Card of Proprietor
	- GST Registration Certificate, if applicable
	- Udyam Registration Certificate (MSME)
	- Business activity proof (any two): land record, trade license, utility bill
	- Proprietor's photograph and signature
Partnership Firm / LLP	- PAN Card of Firm and all Partners
	- Partnership Deed / LLP Agreement
	- GST Registration Certificate

Customer Type	Documents and KYC Requirements
	- Authorization Letter for signatories
	- Recent photographs and signatures of partners/authorized signatories
Private Limited Company	- Certificate of Incorporation
	- PAN Card of Company
	- Memorandum & Articles of Association
	- Board Resolution authorizing account opening and KYC
	- Director's PAN Cards, Aadhaar, and address proof
	- List of Shareholders
	- Beneficial Ownership Declaration: Natural persons holding ≥10% share or control (with their KYC documents)
	- Recent photographs of authorized signatories
Farmer Producer Organisation (FPO)	- Certificate of Registration (Cooperative or Company Law)
	- PAN Card of FPO
	- List of Members / Shareholders
	- Board Resolution authorizing account opening
	- GST or Mandi License, if applicable
	- Beneficial Ownership KYC for individuals holding ≥10% membership or control
Trust / NGO / Association of Persons (AOP)	- Registration Certificate / Trust Deed
	- PAN Card

Customer Type	Documents and KYC Requirements
	- List of Trustees / Managing Committee members
	- Authorization for authorized signatories
	- Beneficial Ownership KYC for significant controlling individuals
	- Registration on DARPAN Portal for NGOs
Others (HUF, Clubs, Societies, Unincorporated Associations)	- Proof of legal existence (e.g., registration certificate, agreement)
	- Proof of operational and registered address
	- KYC documents of authorized signatories
	- Beneficial Ownership verification where applicable
Beneficial Owner(s)	- Declared natural individuals with ownership/control ≥10%
	- PAN card, Aadhaar or equivalent OVD for each beneficial owner
	- Recent photograph and signature
	- Declaration for ownership/control, source of funds
General Points	- Mandatory cross-verification of PAN with CBDT/NSDL database
	- Use of CKYCR KYC Identifier (KYC-ID) for duplicate checking
	- Photocopies must be self-attested and originals verified
	- Video KYC/ V-CIP to be recorded as per RBI standards for digital onboarding
	- Customer consent for data retrieval and storage is mandatory
	- Ensure verification of sanctioned list screening (RBI, FIU, UN, FATF lists)

Customer Type	Documents and KYC Requirements
	- Legal Entity Identifier (LEI) for all entities with credit exposure of ₹5 crore or more.

ARYADHAN FINANCIAL SOLUTIONS PVT. LTD.
NOIDA
UP-201301

****