KYC & PMLA POLICY

(HELPAGE FINLEASE LIMITED)

CIN: L51909DL1982PLC014434

1. Introduction:

The Reserve Bank of India (RBI) has issued a number of circulars and guidelines to ensure that proper Know Your Customer (KYC) norms are followed by NBFCs and that adequate checks and measures are in place to prevent money laundering.

This Know Your Customer and Anti-Money Laundering Policy (Policy) has been framed by **Helpage Finlease Limited** (the "Company") in line with the Master Direction - Know Your Customer (KYC) Direction, 2016 issued by the RBI, as amended from time to time ("KYC Master Directions").

The Company is committed for transparency and fairness in dealing with all stakeholders and in ensuring adherence to all laws and regulations. The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulge any details thereof for cross selling or any other purposes. The Company commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is inconformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with his /her consent and after effective rendering of services.

2. Definitions:

For the purpose of this Policy:

"**Customers or Clients**" means a Person who/which avails any loan funds from Helpage Finlease Limited and includes any corporate and other entities whom Helpage Finlease Limited assists in raising financing through capital market transactions and includes any person who acts of behalf of the Customers or Clients ('Beneficial Owner').

"**Eligibility Criteria**" means eligibility criteria of Helpage Finlease Limited as approved by the Board from time to time.

"**Person**" means has the same meaning assigned in the Prevention of Money Laundering Act, 2002 and includes:

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

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

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

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

"Beneficial Owner" (BO) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means

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

"**Designated Director**" means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money-Laundering Act, 2002 (PML Act) and the Rules.

"**Digital KYC**" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act.

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

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

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

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

"Customer identification" means undertaking the process of CDD

3. SCOPE AND APPLICATION OF THE POLICY

The scope of this policy is:

a) Accepting only those clients whose identity is established by conducting due diligence appropriate to the risk profile of the customer.

b) Reporting to the Financial Intelligence Unit – India (FIU-Ind), or any other agency designated by the Reserve Bank of India, Securities and Exchange Board of India or any other regulatory body, the details of transactions of all or selected clients if and when requested or at regular frequency as may be suggested by such agencies.

c) Cooperating with investigating agencies / law enforcement agencies in their efforts to trace money laundering transactions and persons involved in such transactions.

To fulfil the scope, the following four key elements will be incorporated into our policy:

1. Customer Acceptance Policy (CAP)
2. Customer Identification Procedures (CIP)
3. Monitoring of transactions
4. Risk Management

4. Customer Acceptance Policy (CAP)

The guidelines for Customer Acceptance Policy (CAP) for the Company are given below:

- No account is opened in anonymous or fictitious/ benami name(s).

- The Company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category.

- Accept customers after verifying their identity as laid down in customer identification procedures.

- While carrying out due diligence the Company shall ensure that the procedure adopted shall not result in denial of services to the genuine customers.

- For the purpose of risk categorisation of customer, Company shall obtain the relevant information from the customer at the time of account opening.

- Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk; customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs –as explained in Annex II) may, if considered necessary, be categorized even higher;

- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering (PML) Act, 2002 and guidelines issued by Reserve Bank from time to time;

- The Company shall not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It shall be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

- Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking as there shall be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in the fiduciary capacity and

- Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

- The Company shall prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the Company. However, while preparing customer profile the Company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

- For the purpose of risk categorisation, 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 of low-risk customers would be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher-than-average risk to the bank 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. Banks may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

- Examples of customers requiring higher due diligence may include:
    a) non-resident customers,
    b) high net worth individuals,
    c) trusts, charities, NGOs and organizations receiving donations,
    d) companies having close family shareholding or beneficial ownership,
    e) firms with 'sleeping partners',
    f) politically exposed persons (PEPs) of foreign origin,
    g) non-face to face customers, and
    h) those with dubious reputation as per public information available, etc.

- Adoption of customer acceptance policy and its implementation shall not become too restrictive and shall not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged.

- As advised by RBI under Circular No. DNBS(PD)CC.No.193/03.10.42/2010-11, the Company shall not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the Company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

5. Customer Identification Number (CIN)

Customer identification means identifying the customer and verifying his / her identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain sufficient information such as Voter Id card, PAN number, Passport etc. necessary to establish, to our satisfaction, the identity to each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

It will be ensured that due diligence is observed on the risk profile of the customer in compliance with the extant guidelines in place and the same will be available for verification.

Beside risk perception, the nature of information/ documents required will also depend on the type of customers (individual, corporate etc.)

For customers that are natural persons:

The Company has to obtain sufficient identification data to verify the identity of the customer, his address/location and also his recent Photograph. The Company collects identity proof, bank account details.

For Customers that are legal person or entities, the Company will:

i. Verify the legal status of the legal person/ entity through proper and relevant documents,

ii. Verifying that any person purporting to act on behalf of the legal person/ entity is so authorized and identify and verify the identity of the person and for (i) and (ii) Memorandum of Association and Board Resolution will be collected to ensure that the person purporting to act on behalf of the legal person/ entity is authorised to do so, apart from applicable field/document investigations.

iii. In case of partnership firm, a copy of partnership deed along with the registration certificate of the firm, if registered and power of attorney in favour of person purporting to act on behalf of the firm shall be Collected. In order to authenticate the identity of the person so purporting to represent the Company/Firm, Signature verification/ attestation shall be done either from the banker or copy of passport, driving license or Pan Card to be taken.

iv. Understand the ownership and control structure of the customer and determine who are natural persons who ultimately control the legal person. For this the Company will collect shareholding letter duly certified by the Company Secretary/ Company's Auditor/ Chartered Accountant and Necessary Resolution/ authorization etc.

PERIODIC UPDATION OF KYC

As per the amendment to Master Direction on KYC dated 10th May 2021, the Company has adopted a risk-based approach for periodic updation of KYC in the following manner:

S.NO.	Basis Risk Category	Frequency
1.	High Risk Customers	Once in every two years from the date of opening of the account/ last KYC updation.
2.	Medium Risk Customers	Once in every Eight Years from the date of opening of the account/last KYC updation.
3.	Low Risk Customers	Once in every Ten Years from the date of opening of the account /last KYC updation.

The company shall obtain self-declaration from Individual customers and non- Individual customers of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

In case of change in KYC information of non-individual customer, the Company shall undertake a KYC process which shall be equivalent to on-boarding a new customer.

6. **Monitoring of Transactions**

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company shall prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits, Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. The Company does not accept any deposits. Further, there are no operative accounts where in the need for fixing the threshold limits for individual transactions and aggregate is more relevant and necessary. Most of the Company's loans are EMI based loans on all categories of borrowers. Hence the transactions with the Company are purely shall be restricted to the EMI/loan repayable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI/loan payable, the threshold for turnover shall be restricted to the aggregate EMIs payable year after year. No other transactions what so ever nature other than repayment of loan with interest is carried out by the customer with the Company.

The permanent correct address shall mean the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the Company for verification of the address of the customer. In case utility bill is not in the name of the customer but is close relative: wife, son, daughter and parents etc. who live with their husband, father/mother and son, the Company shall obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) is a relative and is staying with him/her. The Company shall use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, the Company shall keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. 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. The Company shall ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002. It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority.

The Company shall put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation of customers shall be carried out at a periodicity of not less than once in six months. The Company shall also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such

updation shall not be less than once in five years in case of low- risk category customers and not less than once in two years in case of high and medium risk categories.

Maintenance of records of transactions:

The Company shall introduce a system of maintaining proper record of transactions prescribed under rule 3, as mentioned below:

i. all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
ii. all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
iii. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
iv. all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

Preservation of records:

The Company shall maintain the following information in respect of transactions referred to in rule 3:

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it was denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction;

The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, the Company shall maintain for at least ten years from the date of cessation of transaction between the Company and the client, all necessary records of transactions, both domestic or international, which shall permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

The Company shall ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data shall be made available to the competent authorities upon request.

7. **Risk Management**

For effective implementation of KYC policy there will be a proper co-ordination, communication and understanding amongst all the departments of the Company. The Board of Directors shall ensure that an effective KYC program is put in place by establishing proper procedures and ensuring their effective implementation. Heads of all the Departments will ensure that the respective responsibilities in relation to KYC policy are properly understood, given proper attention and appreciated and discharged with utmost care and attention by all the employees of the Company.

The Risk department of the Company will carry out quarterly checks to find out as to whether all features of KYC policy are being followed and adhered to by all the Departments concerned. The Risk Department shall sign off on the KYC documents for corporate entities, before every disbursement.

Company will take steps to ensure that its internal auditors are made well versed with this policy that will carry out regular checks about the compliance of KYC procedures by all the branches of the Company. Any lapse or short coming observed by the internal auditors will be brought to the notice of Department Heads concerned. There will be quarterly assessment to check the compliance level by a committee to be constituted by the Board.

Hiring of Employees and Employee training:

a) Adequate screening mechanism as an integral part of their personnel recruitment/ hiring process shall be put in place.

b) On-going employee training shall be provided to all the employees to adequately train them in AML / CFT and KYC procedures, related policies, regulations and issues.

The inadequacy or absence of KYC standards can subject the Company to serious risks especially reputational, operational, legal and concentration risks.

a) Reputational risk is defined as the risk of loss of confidence in the integrity of the 16 institutions, that adverse publicity regarding the Company's business practices and associations, whether accurate or not causes.

b) Operational risk can be defined as the risk of direct and indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

c) Legal risk is the possibility that law suits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Company.

d) Concentration risk although mostly applicable on the assets side of the balance sheet, may affect the liability as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the liquidity of the Company.

All these risks are interrelated. Any one of them can result in significant financial cost to the Company and diverts considerable management time and energy to resolving problems that arise.

8. **Customer Education**

Implementation of KYC procedures requires the Company to demand certain information from customers which shall be of personal nature or which have hitherto never been called for. This may sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company shall prepare specific literature/pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staffs shall be specially trained to handle such situations while dealing with customers.

9. **Appointment of Compliance/Principal Officer**

The Company has a senior management officer to be designated as Compliance/Principal Officer. Compliance/Principal Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He shall maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The Manager appointed under Companies Act shall be the Compliance/ Principal Officer of the Company for this purpose.

The Company shall abide by all guidelines, directives, instructions and advices of Reserve Bank of India as shall be in force from time to time. The contents in this document shall be read in conjunction with these guidelines, directives, instructions and advices. The Company shall apply better practice so long as such practice does not conflict with or violate Reserve Bank of India regulations.

10. Maintenance And Preservation Of Records

As per the provisions of PMLA, the Company shall maintain records as under:

a) Records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules [referred to in Para 5. Supra] are required to be maintained for a period of ten years from the date of transactions between the Clients and the Company.

b) Records of the identity of all clients of the Company are required to be maintained for a period of ten years from the date of cessation of transactions between the Clients and the Company.

The Company will ensure that the appropriate steps are taken to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copy) that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

11. General

The Company shall ensure that the provisions of PMLA and the Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976, wherever applicable, are adhered to strictly.

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.