Famy Finance Private Limited

Know Your Customer (KYC)/ Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) Policy

Version 1.0

Policy Name	Know Your Customer (KYC)/ Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) Policy
Issue and Effective date	16-05-2024
Date of last review	-
Date of current review	-
Date of next review	As and when required
Periodicity of review	Annual
Owner / Contact	Compliance Group
Approver	Board of Directors
Version	1.0

1. **Introduction** 4
2. **Objective** 4
3. **Key Definitions** 4
4. **Customer Acceptance Policy (CAP)** 6
5. **Customer Identification Procedures** 8
6. **Client Due Diligence (CDD)** 8
7. **Sharing KYC information with Central KYC Records Registry (CKYCR)** 10
8. **Risk categorization of customers** 10
9. **On-going Due Diligence** 11
10. **Periodic Updation of KYC** 12
11. **Record Management** 12
12. **Reporting requirements** 13
13. **Hiring of Employees** 13
14. **Employee training** 14
15. **Mandatory Appointments** 14
16. **Compliance** 14
17. **Policy Review** 15

1. Introduction

Famy Finance Private Limited (hereinafter referred to as 'Famy Finance' or 'the Company' or 'the NBFC') is a non-deposit taking Non-Banking Financial Company (NBFC) duly registered with the Reserve Bank of India ('RBI'). Under the Scale Based Regulatory (SBR) Framework for NBFCs, the Company is categorized as a Base Layer NBFC based on its asset size.

The Company is engaged in the business of carrying out investment and trading activity in various securities such as equity shares, debt securities, futures and options and other financial instruments including derivates as permitted under the applicable regulations as well as lending business.

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

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

2. Objective

The key objectives of the Company are to:

- Prevent criminal elements from using Company for Money Laundering and Terrorist Funding activities.
- Lay out an appropriate eligibility criterion for accepting customers.
- Lay out an effective system for customer identification.
- Effectively manage risks of money laundering, situations that facilitate money laundering, or for the funding of terrorist or criminal activities.
- To enable Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
- Establish adequate monitoring and reporting systems to identify, create and submit timely reports of customer identity, instances or suspicions of fraud, etc. both internally and to appropriate authorities.
- Establish adequate and internal control to ensure proper compliance with all applicable regulations.
- To sufficiently comply with applicable laws and regulatory guidelines.

3. Key Definitions

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

— **Act and Rules** states 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 Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

— **Beneficial Owner**- Beneficial Owner (BO) -

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

i. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b. Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of capital or profits of the partnership.

c. Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.
Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

— **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 RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules

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

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

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

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

d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

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

— **Person** has the same meaning assigned in the Act and includes:

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

— **Suspicious transaction** means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to not have economic rationale or bona-fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

— **Transaction** means any, purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a) opening of an account;
b) entering into any fiduciary relationship;
c) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
d) any payment made or received, in whole or in part, for any contractual or other legal obligation.

4. Customer Acceptance Policy (CAP)

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

a) No account is opened in anonymous or fictitious/benami name.

b) No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

c) No transaction or account-based relationship is undertaken without following the Customer Due Diligence (CDD) procedure set out in this Policy.

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

e) Additional information, where such information requirement has not been specified in this Policy, is obtained with the explicit consent of the customer.

f) REs shall apply the CDD procedure at the individual account level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise.

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

h) CDD Procedure is followed for all the joint account holders, while opening a joint account.

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

j) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by the RBI. The Company shall at all times comply with the requirements of the provisions of the Master Directions on KYC issued by the RBI in this regard.

k) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

l) Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

m) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

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

The CAP shall not result in denial of banking/financial facility to members of general public especially to those who are financially or socially disadvantaged.

Accounts of Politically Exposed Persons (PEPs):

PEPs are individuals who are or have been entrusted with prominent public functions e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The Company shall have the option of establishing a relationship with PEPs provided that:

a. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
b. the identity of the person shall have been verified before accepting the PEP as a customer;

c. the decision to open an account for a PEP is taken at a committee level in accordance with the Customer Acceptance Policy;
d. all such accounts are subjected to enhanced monitoring on an on-going basis;
e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
f. the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

The additional measures applicable to PEP as required under the KYC Directions shall also be applied for family members and close relatives of PEP including the beneficial owners.

5. Customer Identification Procedures

The Company will initiate customer identification under the following circumstances-

- At the start of an account-based relationship with the customer.
- When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on customer due diligence done by a third party, subject to the following conditions:

- Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
- Adequate steps are taken by the Company to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
- The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- The third party shall not be based in a country or jurisdiction assessed as high risk.
- The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

6. Client Due Diligence (CDD)

CDD means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

The details to be collected for conducting CDD of the following types of customers are as under:

5.1 <u>Individual (a beneficial owner, authorised signatory or the power of attorney holder)</u>

For undertaking CDD, the 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) Any one of the following:
   — the Aadhaar number where he decides to submit his Aadhaar number voluntarily; or
   — the proof of possession of Aadhaar number where offline verification can be carried out; or
   — the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
   — the KYC Identifier with an explicit consent to download records from CKYCR;

b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company.

5.2 Sole Proprietary Firm

For opening an account in the name of a sole proprietary firm, the following shall be obtained:

a) CDD of the individual (proprietor) as above; and

Any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm:

b) Registration certificate including Udyam Registration Certificate (URC) issued by the Government;
c) Certificate/licence issued by the municipal authorities under Shop and Establishment Act;
d) Sales and income tax returns;
e) CST/VAT/ GST certificate;
f) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities;
g) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute;
h) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities;
i) Utility bills such as electricity, water, landline telephone bills, etc.;

Note - In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company, at its discretion, accept only one of those documents as proof of business/activity, provided the Company undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

5.3 Company

For opening an account in the name of a company, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Certificate of incorporation;
b) Memorandum and Articles of Association;
c) Permanent Account Number of the company;
d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
e) CDD at the individual level, relating to beneficial owner;
f) the names of the relevant persons holding senior management position; and
g) the registered office and the principal place of its business, if it is different.
h) Mailing address and telephone number of the company
i) List of shareholders (promoter shareholding identified separately)
j) List of Directors Including promoter directors
k) Brief note about the company and its business

5.4 Partnership firm

For opening an account in the name of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Registration certificate;
b) Partnership deed;
c) Permanent Account Number of the partnership firm;
d) CDD at the individual level, relating to beneficial owner,;
e) the names of all the partners; and
f) address of the registered office, and the principal place of its business, if it is different.
g) brief note about the partnership firm

5.5 Trust

For opening an account in the name of a trust, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Registration certificate;
b) Trust deed;
c) Permanent Account Number or Form No.60 of the trust;
d) CDD at the individual level, relating to beneficial owner;
e) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust;
f) the address of the registered office of the trust; and
g) list of trustees and documents, at the individual level, for those discharging the role as trustee and authorised to transact on behalf of the trust.

7. Sharing KYC information with Central KYC Records Registry (CKYCR)

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

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

ii. It must be ensured that, in terms of provision of Rule 9(1A) of the PML Rules, the Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

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

8. Risk categorization of customers

The Company shall have a risk-based approach which includes the following.

a. Customers shall be categorised as low, medium and high-risk category or any other category decided by risk management commitee, based on the assessment and risk perception of the Company

b. The indicative parameters that the Company may factor in for the purpose of risk-categorisation of customers are:

   i. customer's identity,

   ii. nature of business activity,

   iii. information about the customer's business and location,

   iv. geographical risk covering customers as well as transactions,

   v. type of products/services offered,

   vi. delivery channel used for delivery of products/services,

   vii. types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc.

   viii. the ability to confirm identity documents through online or other services offered by issuing authorities.

c. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

9. On-going Due Diligence

- The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
- The extent of monitoring shall be aligned with the risk category of the customer. For example, high risk accounts have to be subjected to more intensified monitoring.
- Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:
    - Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
    - Transactions which exceed the thresholds prescribed for specific categories of accounts.
    - High account turnover inconsistent with the size of the balance maintained.
    - Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.
- A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
- The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

10. Periodic Updation of KYC

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

In case of no change in KYC information: In case of no change in the KYC information of the customer, a self-declaration in this regard shall be obtained from the customer through its email id registered with the Company, letter from an official authorized by the customer in this regard, board resolution, etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with it is accurate and shall update the same, if required, to keep it as up-to-date as possible.

In case of change in KYC information: In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

In addition to the above, the Company shall ensure that,

- The KYC documents of the customer as per the current CDD standards are available. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.

Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

11. Record Management

The Company shall ensure to:

- maintain all necessary records of transactions between the Company and the customer, for at least five years from the date of transaction.
- preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
- make available swiftly, the identification records and transaction data to the competent authorities upon request;
- introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
  - the nature of the transactions;
  - the amount of the transaction and the currency in which it was denominated;
  - the date on which the transaction was conducted; and
  - the parties to the transaction.

- 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;
- maintain records of the identity and address of their customer, and records in respect of transactions referred to in PML Rule 3 in hard or soft format.

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

12. Reporting requirements

To Financial Intelligence Unit – India (FIU-IND)

The Company shall establish a robust software (either developed inhouse or purchased) which send alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

The Principal Officer of the Company shall report to the Director, FIU-IND the following:

- Cash Transaction Reports (CTR) in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of PML R rule 3 every month by the 15th day of the succeeding month.
- Suspicious transactions and transactions referred to in clause (D) of sub-rule (1) of PML Rule 3 not later than 7 working days on being satisfied that the transaction is suspicious.
- the information in respect of transactions referred to in clause (F) of sub-rule (1) of PML Rule 3, every quarter by the 15th day of the month succeeding the quarter.

Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

The Company shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

Further, the Company, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director, FIU-IND is confidential.

To Ministry of Home Affairs (MHA)

- Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under Unlawful Activities (Prevention) (UAPA) Act, 1967 notification dated 122February 2, 2021.

13. Hiring of Employees

The Company shall:

- put in place an adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process.
- endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective

communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally.

- strive to develop an environment which fosters open communication and high integrity amongst the staff.

14. Employee training

The Company shall:

- Put in place an on-going employee training programme so that the relevant members of staff are adequately trained in KYC/AML/CFT policy.

15. Mandatory Appointments

The Company shall ensure to designate and appoint, with the approval of the Board, two separate individuals as a principal Officer and Designated Director of the Company.

Principal Officer

A Principal Officer means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.

- The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
- The name, designation and address of the Principal Officer shall be communicated to both the FIU-IND and to the RBI.

Designated Director

A "Designated Director" is a director nominated to act, as required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules). It shall include a Managing Director or a whole-time Director duly authorized by the Board of Directors of the Company.

- The Designated Director shall ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.
- The name, designation and address of the Designated Director shall be communicated to both the FIU-IND and to the RBI.

Senior Management

To be in compliance with obligations provided under the PML Act, the Senior Management shall be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. In this regard, the senior management of the Company ("Senior Management") shall comprise of the key managerial personnel as defined under Companies Act, 2013

16. Compliance

The key responsibilities of Board of Directors to ensure strict compliance of the Policy include ensuring:

- Independent evaluation of the compliance functions of Policy and procedures, including legal and regulatory requirements.
- Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
- Submission of quarterly audit notes and compliance to the Audit Committee.
- Ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

17. Policy Review

The Board of Directors shall provide for periodical review of the compliance and the functioning of the KYC/AML/CFT Policy by the senior management specified above.

The Company will review the policy at least once in a year or earlier, in the following scenarios:

a) In case of any changes impacting the business operations of the Company, or
b) Any changes in the regulatory framework applicable to the Company.

Any modifications made to the Policy will be approved by the Board and communicated to all relevant departments across the organisation.