KYC & AML/ CFT POLICY OF MONEYSUKH ADVISORS IFSC LLP

Document Control	
Title	KYC & AML/ CFT Policy
Policy Owner	Designated Partners
Execution Team	Compliance Officer
Approved by	Designated Partners
Version	V3
Tentative next review	On any Regulatory change or Annual, whichever is earlier

Version Summary

Version	Updates	Review Date	Prepared by Department	Approved by
V3	Third Policy	16.05.2026	Compliance	Designated Partners

Table of Contents

1. INTRODUCTION 4
2. SCOPE, APPLICATION AND OBJECTVE 4
3. NEED FOR POLICY 5
4. DEFINITION 8
5. DESIGNATED DIRECTOR AND PRINCIPAL OFFICER 11
6. RISKS OF NON-COMPLIANCE TO THE LAWS AND REGULATIONS 12
7. KNOW YOUR CLIENT AND ANTI MONEY LAUNDERING POLICY 13
8. CLIENT IDENTIFICATION PROCEDURE ("CIP") 13
9. CLIENT DUE DILIGENCE (CDD) 17
10. CLIENT'S ACCEPTANCE POLICY 28
11. RISK – BASED APPROACH ("RBA") 30
12. BUSINESS FACILITATOR 37
13. RECORD KEEPING & RETENTION OF RECORDS 37
14. MONITORING OF TRANSACTIONS 38
15. REPORTING OF SUSPICIOUS TRANSACTIONS TO FIU IND 40
16. COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS 41
17. PAYMENT TRANSPARENCY STANDARDS 44
18. AUDIT, EMPLOYEES HIRING & TRAINING 46
19. INVESTORS EDUCATION 47
20. ANNEXURE – I CLIENT RISK ASSESSMENT PROCDEURE 51
21. ANNEXURE – II DIGITAL KYC PROCESS FOR INDIAN NATIONALS 52

1. INTRODUCTION

Moneysukh Advisors IFSC LLP (hereinafter referred to as "the LLP"), is a Fund Management Entity regulated by International Financial Services Centres Authority and is acting as an Investment Manager of existing fund and funds that may be launched in the future. This policy is drafted in compliance of the International Financial Services Centres Authority (IFSCA) (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 ("IFSCA (AML/CFT and KYC) Guidelines").

The LLP being a Regulated Entity requires compliance with Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) laws of the IFSC, for the investors of the Regulated Entities it deals with along with the adherence to international practices recommended by Financial Action Task Force the LLP has developed the following KYC & AML/CFT Policy in compliance with the applicable laws and any other regulation, rules, guidelines as may be in force from time to time.

2. SCOPE, APPLICATION AND OBJECTIVE

This Policy applies to the LLP, Funds/Schemes managed by the LLP, Partners, Designated Partners and officers of the LLP, the business facilitators, the administrators and those involved in AML/CFT processes, on-boarding of Investors and upon performance of any compliance activities as a fund manager and further including any of the person authorized to act on behalf of the LLP. All aforementioned persons to be referred as "**Concerned Persons**". The Policy and the annexures thereto are approved by the designated partners of LLP and are confirmed by the Business Facilitator of the LLP.

The objective of the KYC & AML Policy is to prevent the LLP from being used, intentionally or unintentionally, by criminal elements for money laundering activities and terrorist financing. KYC procedures also enable the LLP to know/understand its clients and their financial dealings better, which in turn help the LLP to manage its risks prudently. Also, maintenance of records of the transactions as prescribed forms part of the Policy.

Information collected from the Investors shall be kept confidential and the LLP shall not divulge any details thereof for cross selling or any other purposes. Information sought from the client shall be relevant to the perceived risk, shall not be intrusive, and shall be in conformity with the guidelines issued or laws of the land from time to time. Any other information from the client shall be sought separately with his /her consent.

Hence, this Know Your Client (KYC) and Anti-Money Laundering (AML) Policy ("the Policy") has been implemented in a manner to adhere with the AML/CFT requirements of IFSCA ("the Authority") for IFSC jurisdiction and for other jurisdictions as well. However, where the law of another jurisdiction does not permit the implementation of KYC/AML-CFT standards that are equivalent to or higher than those that apply to the LLP incorporated in an IFSC, the LLP or the Regulated Entity shall: -

(i) inform the Authority in writing; and

(ii) apply appropriate additional measures to prevent the ML/TF risks posed by the relevant branch or subsidiary.

The objective of KYC Policy is to:

a. Prevent the LLP or its Schemes from being used, intentionally or unintentionally, by criminal elements for money laundering activities.
b. To enable to know/understand the Investors and their financial dealings better which in turn helps understanding the risks associated with the dealings of the Investors.
c. To assess the ML/TF risks presented by the Investors.
d. To verify the identity, suitability, and risks involved with maintaining a business relationship with the Investors.
e. To adopt and implement KYC, AML and Combating of Financing of Terrorism (CFT) standards in its day-to-day practice.
f. To have a proper Customer Due Diligence (CDD) process before registering Investors.
g. To monitor and report suspicious transactions.
h. To ensure the transparency and availability of beneficial ownership information of legal persons and arrangements; and
i. To maintain records of all transactions as required under the applicable Laws.

3. NEED FOR POLICY

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. As a duty of a regulated entity of IFSCA AML/CFT and KYC policy is to be framed under the IFSCA (AML/CFT and KYC) Guidelines.

To ensure compliance with this Policy, it is important to understand the meaning of Money Laundering ("ML") and Terrorist Financing ("TF") as follows:

Money Laundering ["ML"] is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over the proceeds and, ultimately, to provide a legitimate cover for their source of income/wealth.

ML does not only constitute of activities that are associated to organised crime and drug trafficking but also includes any person who deals with another person's direct or indirect benefit from crime.

Illegal arms sales, smuggling, and the activities of organised crime, including for example, drug trafficking can generate huge profits. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through ML.

ML is a global phenomenon that affects all countries in varying degrees. By its very nature, it is a hidden activity and therefore the scale of the problem and the amount of criminal money being generated either locally or globally each year is impossible to measure accurately. However, failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime a more attractive proposition.

Under the AML/CFT recommendations of FATF both the act of laundering money and conspiracy to commit ML is a criminal offence and measures has to be taken by all financial services sector entities to prevent such activities. Section 3 of The Prevention of Money-Laundering Act, 2002 ("Act") define the offence of money-laundering as follows:

Offence of money-laundering: Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering.

Explanation: a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely:

(a) concealment; or
(b) possession; or
(c) acquisition; or
(d) use; or
(e) projecting as untainted property; or
(f) claiming as untainted property, in any manner whatsoever;
(g) the process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.

Terrorist Financing ["TF"] refers to the act of providing financial and/or technical support to acts of terror, terrorists, or terrorist organisations to enable them to carry out their criminal activities. The aim of the measures taken by the regulatory authorities is to identify, trace and curb terrorist financing.

TF is an activity that promotes illegal acts and involves legitimately, or illegitimately derived property used to support terrorism.

The AML/CFT legislation also incriminates acts of omission leading to ML & TF.

To combat both ML and TF, the LLP has implemented Client Due Diligence measures at both commencement and ongoing basis of every relationship. Further, an assessment of risk should always be documented, reasonably and objectively justifiable and sufficiently robust.

Phases in the Money Laundering Cycle

To identify, understand and accurately assess the ML/TF/PF evasion risks to which we may be exposed at both the enterprise and business relationship levels, we must be aware of the three phases of money laundering. The paragraphs below describe the crime of money laundering as consisting of three distinct (though sometimes overlapping) phases.

Placement

During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international.

Examples of placement transactions are:

- Blending of funds: commingling of illegitimate funds with legitimate funds, such as placing the cash derived from criminal activities into cash-intensive, locally owned businesses
- Foreign exchange: purchasing of foreign exchange with illegal funds
- Breaking up amounts: placing cash in small amounts and depositing them into numerous bank accounts to evade reporting requirements
- Currency smuggling: cross-border physical movement of cash or monetary instruments
- Loans: repayment of legitimate loans using laundered cash

Layering

This second phase involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds. It is about the separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.

Examples of layering transactions are:

- electronically moving funds from one country to another and dividing them into advanced financial options and/or markets
- moving funds from one financial institution to another or within accounts at the same institution
- converting the cash placed into monetary instruments
- reselling high-value goods and prepaid access/stored value products
- investing in real estate and other legitimate businesses
- placing money in stocks, bonds, or life insurance products
- using shell companies to obscure the ultimate beneficial owner and assets

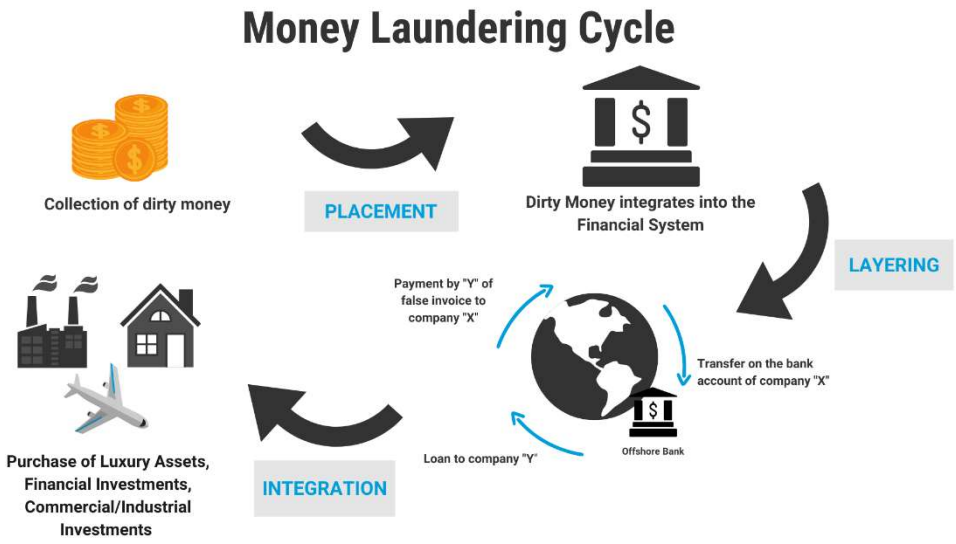
Integration

This phase entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures, or luxury assets. By the integration phase, it is exceedingly difficult to

distinguish between legal and illegal wealth. This phase provides a launderer the opportunity to increase his or her wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or LLP's legitimate employment, business or investment ventures and a person's wealth or a LLP's income or assets. It is about supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

Examples of integration transactions are:

- purchasing luxury assets, such as property, artwork, jewellery, or high-end automobiles
- early reimbursement of mortgages or loans
- early redemption of investments in collective investment funds, insurance linked investment products, discretionary managed portfolios
- getting into financial arrangements or other ventures where investments can be made in business enterprises



4. DEFINITION

1. "Act" and "Rules" means the Prevention of Money-laundering Act, 2002 and the Prevention of Money laundering (Maintenance of Records) Rules, 2005, respectively.

2. "Business Facilitator" means a person authorised by the LLP, to verify the information/officially valid documents provided by the client for opening account with it.

3. "Certified Copy" means comparing the original officially valid document provided by the client with the copy thereof and recording the same as 'true copy' by the authorised officer of the Regulated Entity. Provided that in case of non-resident individuals including Non-Resident Indians (NRIs), the certification may be carried out by:

i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship;
ii) Notary Public (outside India);
iii) Court Magistrate (outside India);
iv) Judge (outside India);
v) Certified public or professional accountant (outside India);
vi) Lawyer (outside India);
vii) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or
viii) Any other authority as may be specified by the Authority.

4. "LLP" or "Regulated Entity" for the purpose of this policy shall mean the IFSCA registered Fund Management Entity.

5. "Customer" or "Client" for the purpose of this policy shall mean a person or investor who is engaged in a financial transaction or activity with the LLP or with the Schemes managed and includes a person on whose behalf the person engaged in the transaction or activity, is acting.

6. "Business Facilitator" for the purpose of this policy shall mean Moneysukh Advisors IFSC LLP (Name of the entity providing Investor on-boarding services)the Entity, registered under the IFSCA as an authorized Ancillary Service Provider acting as a Business Facilitator.

7. "Officially Valid Document" means the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card issued by the Election Commission of India or letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator;

Provided that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document.

Provided further that, where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be 'officially valid document':

a) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

b) letter issued by a gazetted officer, with a duly attested photograph of the person.
Provided also that, where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document shall also be deemed to be Officially Valid Document:

(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, Municipal tax receipt, city council tax receipt, or such other equivalent document;
(iii) Post Office savings bank account statement or statement of a bank account including of a foreign bank;
(iv) 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.

Provided also that in case the Officially Valid Document 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;

However, in case of a foreign national categorized as Medium/ High risk customer, the latest utility bill or bank statement cannot be accepted as an address proof.

Provided also that where the client submits his proof of possession of Aadhaar number as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authority of India.

8. "Politically Exposed Person" means the individuals who are or have been entrusted with prominent public functions by any country, which shall include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or International Organisation Politically Exposed Person.

9. "Senior Management" means:

(a) In relation to a Regulated Entity,
(i) for an incorporated entity in International Financial Services Centre in India, every member of the Regulated Entity's Governing Body;
(ii) for a branch, the person or persons who control the day-to-day operations of the Regulated Entity in an IFSC and may include such other persons as may be designated by the Regulated Entity.
(b) In relation to a customer, that is a legal person, every member of its Governing Body and the person or persons who control its day-to-day operations.

10. "Third Party" means

(a) A financial institution which is subject to and supervised by a financial regulator; or
(b) In relation to a Regulated Entity, its branches, subsidiaries, parent entity, the branches and subsidiaries of the parent entity, and other related corporations;

AND

(c) Has an existing client relationship with a person whose data would be used for CDD and customer verification by a Regulated Entity.

5. DESIGNATED DIRECTOR AND PRINCIPAL OFFICER AND SENIOR MANAGEMENT

- To be in compliance with these obligations, our senior management is fully committed for establishing appropriate policies and procedures for the prevention of ML, TF and Bribery and Corruption and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

- The LLP has appointed the Designated Director who shall be responsible for to ensure overall compliance with the obligations imposed under the Act, the Rules, IFSCA Guidelines and this Policy.

- The LLP has appointed/designated two different Individuals as Designated Director and Principal Officer to enable unbiased judgments and facilitate impartial advice to management. Further, the Principal Officer is distinct from the internal audit and business line functions.

- The LLP has designated the Principal Officer who shall be responsible for implementation and compliance of this policy and shall undertake the following responsibilities:
  - Assist with the implementation of the LLP's KYC and AML/CFT and procedures are review them at least annually to evaluate their effectiveness and whether the policy or related procedures should be revised to respond to any apparent or actual weaknesses; and
  - Interact with and assist the employee on the implementation of the day-to-day operation of the KYC and AML/CFT Policy;
  - carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with this Policy;
  - promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters within the organisation.
  - informing employees, officers and representatives promptly of regulatory changes.
  - ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected.
  - reporting or overseeing the reporting of suspicious transactions.
  - advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;
  - reporting to senior management on the outcome of reviews of the Regulated Entity's compliance with these Guidelines & risk assessment procedures; and
  - reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection & compliance reviews to the Regulated Entity's senior management.
  - The business interests of an LLP should not interfere with the effective discharge of the above-mentioned responsibilities of the Principal Officer and potential conflicts of interest should be avoided.

- To report any suspicious transactions to the FIU in the manner described by the FIU and to attend to queries from the FIU.
- To report annually (or on such frequency requested by the Designated Partners) and make such other periodic reports as he/she deems necessary to the Designated Partners of the LLP dealing with:
  - the number of internal reports made by employee, and
  - the number of reports made to the FIU.
- To enable unbiased judgments and facilitate impartial advice to management, the Principal Officer should be distinct from the internal audit and business line functions. Where any conflict between business lines and the responsibility of the Principal Officer arises, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the LLP's management.

The Senior Management approval wherever required will include approval from any two of the Designated Partner's or One Designated Partner and Principal Officer of the FME.
The Approval accorded from the Senior Management shall be post facto noted at the ensuing meeting of Designated Partners of the LLP from time to time. Similarly, all the reporting to the senior management under this Policy shall be undertaken.

6. RISKS OF NON-COMPLIANCE TO THE LAWS AND REGULATIONS

Failure to comply with the AML/CFT Legislation may result to the following risks:

Regulatory and Compliance risk: Failure to comply with the AML/CFT Legislation may lead to regulatory actions and depending on the severity of the breach, it may result in revocation of a licence of a business and the LLP may be subject to fines and penalties.

Reputational risk: Failure to comply with the AML/CFT Legislation may result in reputational repercussions, which eventually leads to distrust: clients may leave, new customers may be put off and potentially beneficial partnerships may never develop.

Financial risk: Penalties and fines resulting from regulatory actions, revocation of licence and/or loss of business due to damage of reputation may cause the LLP face financial distress.

Operational risk: The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.

A risk-based approach towards the prevention and detection of ML and TF aims to support the development of preventative and mitigating measures that are commensurate with the ML and TF risks identified by the LLP.

7. KNOW YOUR CLIENT AND ANTI MONEY LAUNDERING POLICY

Know Your Client or KYC, as popularly known across the industry, is the process of identifying a client before signing him/her as an investor under a specific fund. KYC norms mandate Financial Institutions and Financial Intermediaries to obtain and verify personal and contact

information of their clients in accordance with the laid down norms. Regardless of the amount invested, KYC is mandatory for all applications.

The LLP has framed its KYC & AML Policy in lines with the KYC/AML Policy of its Business facilitator by incorporating the following Six key elements:

i Risk Based Approach and Risk Assessment
ii Client Identification Procedure
iii Client Due Diligence Procedure
iv Client Acceptance Procedure
v Monitoring of Transactions / On-going due diligence;
vi Training and Awareness of Employees and Investors

The LLP reserves a right to suspend or discontinue the service in case client fails to provide KYC information as may be required to identify the Client. Further, LLP will not be held responsible for any discontinuance of service for those clients who have not submitted the KYC information as required to the LLP.

The LLP has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. It is crucial that all those concerned fully understand the rationale behind the KYC & AML policies and implement it consistently.

8. CLIENT IDENTIFICATION PROCEDURE ("CIP")

8.1 If a customer is a natural person, the LLP shall obtain at least the following information:

a) Full name, including any aliases;
b) Unique Identification Number (such as an Identity card number, passport number, etc.);
c) Date of birth;
d) Nationality;
e) Legal domicile;
f) Current residential address; (other than a post office box address);
g) Contact details such as personal, office or work telephone numbers.

8.2 If a customer is a legal person or legal arrangement, the LLP shall obtain at least the following information:

The full name and any trading name;
a) Unique identification Number (i.e., Tax identification number or equivalent where this exists, incorporation number or business registration number);
b) Registered or business address, and if different, its principal place of business;
c) Date of establishment, incorporation or registration;
d) Place of incorporation or registration.

8.3. Further, in cases where the customer is a legal person or legal arrangement, the LLP shall also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. In addition to this, the LLP shall also identify and screen the related

parties or connected parties of such customer and should remain apprised of any changes to connected parties. For identification of the connected parties, the LLP shall obtain at least the following information of each related or connected party:

a) full name, including any aliases; and
b) Unique Identification Number (such as an Identity card number, passport number, etc.)

The concept of domicile generally refers to the place which a person regards as his permanent home and with which he has the closest ties, or which is his place of origin. The LLP shall exercise greater caution when dealing with an unfamiliar or a new customer.

Apart from obtaining the identification information required under Clause 7 the LLP shall (if not already obtained as part of its account opening process) also obtain additional information on the customer's background such as occupation, employer's name, nature of business, range of annual income, other related accounts with the LLP and whether the customer holds or has held a prominent public position. Such additional identification information enables the LLP to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the account.

Identification of connected parties or related parties may be undertaken using publicly available sources or databases such as LLP registries, annual reports. Additionally, it could be based on substantiated information provided by the customers.

8.4. Verification of Identity of Customer

The LLP has appointed a service provider who shall act as a Business Facilitator in accordance with the agreement entered along with the terms and conditions ensuring customer secrecy and data protection for verifying the information/OVD provided by the Client for opening account.

The LLP/ Business Facilitator shall verify the identity of the client using reliable, independent source data, documents or information. Where the Client is a legal person or legal arrangement, a Regulated Entity shall verify the legal form, proof of existence, constitution and powers that regulate and bind the client, using reliable, independent source data, documents or information.

When relying on documents, the LLP/ Business Facilitator understands that the most reliable documents to verify the identity of the Client are those which are most difficult to obtain illegally or to counterfeit. These may include government-issued identity cards or current valid passport, reports from independent LLP registries, published or audited annual reports and other reliable sources of information. The rigor of the verification process should be commensurate with the customer's risk profile.

In verifying the identity of a Client, the LLP may obtain the following documents:

In case of Natural Persons –

a) any of the OVD specified under this Policy that contains photograph of the customer, name, unique identification number, date of birth and nationality; and
b) Residential address based on OVD or recent utility bill, bank statement or such other documents specified under the definition of OVD.

In case of Legal persons or Legal Arrangements-

a) Name, legal form, proof of existence and constitution: - the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/agreement, trust deed, constitutional document, certificate of registration or any other document from a reliable independent source; and

b) Powers that regulate and bind the legal person or legal arrangement: - This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement and resolution of the LLP or similar document authorising the opening of an account and appointment of its authorised signatories.

In cases where a customer is a natural person, the LLP shall obtain the OVD that contain a clear photograph of that customer.

In cases where a customer is a foreign national, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national would also be considered as OVD. In case where the customer is an Indian national, OVD shall include the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card, etc. as prescribed under the Rules (For more detailed understanding, refer OVD definition). For the purpose of customer verification, equivalent e-documents of OVDs shall also be treated as original document by the LLP or Business Facilitator

In cases where other than simplified measures are applied, the customer shall submit updated OVD or their equivalent e-documents thereof with current address within a period of three months of submitting the documents specified hereinabove.

Explanation: - For those customers to whom simplified measures are not applied, the bank account or Post Office savings bank account statement or statement of foreign bank shall not be accepted as deemed OVD for the limited purpose of proof of address.

While undertaking CDD for different customers (including legal persons or legal arrangements), the LLP should obtain such information and documents as required under these Guidelines. A list of information and documents which should be obtained for onboarding customers shall be prepared by the LLP under the applicable IFSCA Guidelines and basis the requirement of LLP from to time and shall be maintained, reviewed and updated along with this Policy.

Further, for onboarding Indian Nationals, the LLP may follow the procedure as specified under Annexure-II of the AML/CFT Guidelines as provided in the Policy.

A Regulated Entity shall examine the original identification documents and retain a copy of the same. However, in complying with Clause 9 (i.e., undertaking customer due diligence), at times, if a customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where Regulated Entity has no physical contact with the customer or the onboarding of customer is done through non-face to face mode), the LLP should obtain a copy of the document that is certified to be a 'true copy' and such certification may be carried out by person specified in this Policy.

The LLP shall ensure that documents obtained for performing CDD, as required under this Policy, are clear and legible. This is important for the establishment of a customer's identity, particularly in situations where business relations are established through non-face to face mode.

Except for high-risk customers, the following mode of verifications is also considered as sufficient to satisfy the requirements of **Clause 7:**

- downloading publicly available information from an official source (such as a regulator's or other official government website);

- CDD information and research obtained from a reputable LLP or information obtained from reliable and independent public information found on the internet and commercial databases, provided that the commercial database is recognized for such purpose by the home regulator, if any, of the database.

Where the LLP obtains data, documents or information from the customer or a third party, it shall ensure that such data, documents or information is up-to-date.

Where the customer is rated as high-risk, the identification information shall be independently verified, using both public and non-public sources.

8.5. Identification and Verification of Identity of Natural Person appointed to act on behalf of Customer:

a) Where a customer is a natural person or legal person and appoints one or more natural persons to act on its behalf for establishing business relations with a Regulated Entity, the LLP shall identify each natural person who acts or is appointed to act on behalf of such natural or legal person by obtaining information as specified in Clause 7.1. above.

b) Further, the LLP shall verify the identity of each such natural persons using reliable, independent source data, documents or information. Furthermore, the LLP shall verify the authorisation of each natural person appointed to act on behalf of the customer by obtaining at least the following:

   i The appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf which may include power of

attorney, resolution passed by Governing Body or authorisation granted to transact on its behalf.

ii Where there is a long list of natural persons appointed to act on behalf of the customer (e.g., a list comprising more than 10 authorized signatories), the LLP shall verify those natural persons who will deal directly with the Regulated Entity.

8.6. Identification and Verification of Identity of Beneficial Owners

Where there is one or more Beneficial Owners in relation to a customer, the LLP shall identify the Beneficial Owners and take reasonable measures to verify their identities using the relevant information or data obtained from reliable, independent sources.
For the identification and verification of Identity of Beneficial Owner, the LLP should consider the following in relation to:

a) Customers that are legal persons

i) The identity of the natural person(s) (whether acting alone or together) exercising control over the legal person through ownership or who ultimately owns the legal person;

ii) To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural person(s) (if any) who ultimately control the legal person or have ultimate effective control over the legal person.

b) Customers that are legal arrangements

i) 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 ten per cent. 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.

ii) In all other types of legal arrangements, the LLP shall identify persons in equivalent or similar positions.

9. CLIENT DUE DILIGENCE (CDD)

The Client Due Diligence (CDD) measures comprise the following:

The LLP or Business Facilitator after assigning risk rating for each Client proportionate to their AML/CFT risks, shall undertake the Client Due Diligence. While undertaking the CDD, a LLP/ Business Facilitator shall:

i) undertake Client Due Diligence measures as detailed under Clause 9.1, in respect of all the Clients;

ii) undertake Enhanced Client Due Diligence measures as detailed under Clause 9.2, in addition to the CDD measures detailed under Clause 9.1, in respect of the Client who has been assigned 'high risk'; and,
iii) Undertake Simplified Client Due Diligence measures as detailed under Clause 9.3 by modifying Client Due Diligence process detailed under Clause 9.1, in respect of a Client who has been assigned 'low risk'.

9.1. Client Due Diligence Requirements for undertaking Client Due Diligence (CDD)

In undertaking Client Due Diligence the following measures shall be undertaken by a LLP:

a) Identifying the client and verifying that client's identity using reliable, independent source documents, data or information.
b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a manner that the Regulated Entity is satisfied that it knows who the beneficial owner is.
   Similarly, for legal persons and arrangements, the CDD shall include taking reasonable steps to understand the nature of the client's business, its ownership and control structure.
c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Regulated Entity's knowledge of the client, client's business and risk profile, including, where necessary, the source of funds.

9.2. Parameters to Identify and Verify the Identity of Beneficial Owners:

Where the client is not a natural person, the LLP shall understand the nature of the client's business, its ownership and control structure, before opening an account.

9.2.1. Beneficial Owner Identification:

a) Where the client 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 or entitlement to more than **ten per cent**. of the shares or capital or profits of the LLP;
   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 client 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 **ten per cent.** of capital or profits of the partnership or who exercises control through other means;

Explanation - For the purpose of this clause, "Control" shall include the right to control the management or policy decision;

c) Where the client 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 or entitlement to more than **fifteen per cent**. of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (c) above, the beneficial owner is the relevant natural person who holds the position of **senior managing official**.

d) Where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with **ten per cent**. 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.

9.2.2. Unless the LLP or Business Facilitator has doubts about the veracity of the CDD information, or suspects that client may be connected with ML/TF, it shall not be required to identify and verify the identity of any shareholder or beneficial owner of a client, where the client or the owner of the controlling interest is an entity listed on the stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities and such other entities who have been excluded from the requirements regarding identifying and verifying beneficial owners of a client under the Act and Rules.

9.2.3 As per the proviso of rule 9(1)(b) of the Rules, in cases where a client is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a LLP incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in sub-rules (3) to (9) of the rule 9 of the Rules shall be applicable for due diligence of such beneficial owner.

9.2.4. A Regulated Entity may also consider obtaining an undertaking or declaration from the client on the identity of, and the information relating to, the beneficial owner in the format of the LLP or in such format that it includes all the possible details to identify the Beneficial Owners.

9.2.5. Notwithstanding the obtaining of such an undertaking or declaration, the Regulated Entity remains responsible for complying with the obligations under the Guidelines to take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the client.
Where the client has submitted any documents for the purpose of client due diligence it shall submit to the Reporting entity any update of such documents, for the purpose of updating the records, within 30 days of such updation.

9.2.6. Where the customer is not a natural person and has a complex ownership or control structure, a Regulated Entity should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.

9.3. Where the Regulated Entity has exhausted all possible means but has not been able to identify the Beneficial Owners under **Clause 9.2., it shall treat the Senior Management** of the said legal person or legal arrangement, as the Beneficial Owners. However, in such cases, the Regulated Entity shall keep a record of all the actions it has taken to identify the Beneficial Owners of such legal persons or legal arrangement.

9.4. If the ownership or control arrangements of a client are of such a nature that the Regulated Entity is prevented from identifying the Beneficial Owners, the Regulated Entity shall establish a business relationship with the client under **Clause 10.3. of this Policy**

9.5. In relation to Clause 9.2.2. and Clause 9.2.3. above, currently as on the date of this Policy, the notified jurisdictions by Central Government are as follows: -
(i) United States of America
(ii) Japan
(iii) South Korea
(iv) United Kingdom excluding British Overseas Territories
(v) France
(vi) Germany
(vii) Canada

9.6. Information on the Purpose and Intended Nature of Business Relations

a) A Regulated Entity shall, while establishing business relationship, understand and as appropriate, obtain information from the client as to the purpose and intended nature of business relations.
b) The measures taken by a Regulated Entity to understand the purpose and intended nature of business relations should be commensurate with the risk profile and complexity of the client's business.

9.7. Accounts of Politically Exposed Persons

Politically Exposed Persons Risk or "PEP" risk relates to the risks associated with providing financial and business services to government ministers or officials from countries with widely known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have anti-money laundering standards, or where these do not meet international financial transparency standards. The LLP's business could face considerable reputational damage if the LLP is found to have a business relationship with client involving the proceeds of corruption.

Therefore, the transactions by PEPs should be subject to closer scrutiny. The LLP must consider the degree of ownership, the prominence of the individual PEP and their past history, performance track record or reputation, their public responsibilities and duties, potential conflicts of interest, the likelihood that political changes in the country could expose

wrongdoing by the PEP and their source of wealth and source of funds must be established as legitimate both at outset and on an ongoing basis.

a) The LLP/ Business Facilitator shall determine if a client or any natural person appointed to act on behalf of the client, or any beneficial owner of the client is a politically exposed person (PEP) or in case of a life insurance or other similar policy, if a beneficiary of the policy, or a Beneficial Owner of a beneficiary, is a PEP. To determine that same the Regulated Entity shall take declaration stating whether the Client is a PEP or is related to a PEP at the on-boarding and on periodical basis.

b) The LLP/ Business Facilitator shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a client or any beneficial owner of the client or beneficiary of a life insurance or other similar policy, or a Beneficial Owner of a beneficiary is determined by the Regulated Entity to be a PEP:
    i) Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family members, any beneficial owner and close relatives;
    ii) Verify the identity before accepting the PEP as a client;
    iii) Obtain approval from its Senior Management before opening an account of a PEP or making any payout under the life insurance or other similar policy to the PEP;
    iv) In the event of an existing client or the beneficial owner of an existing account subsequently becoming a PEP, obtain the Senior Management's approval to continue the business relationship;
    v) Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the client's transactions or activities appear unusual or suspicious.
    vi) Carry out the additional Client Due Diligence for circumstances specified in sub-clauses (i) to (v) above, before making any payout under the life insurance or other similar policy.

c) The LLP may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for:-
    i) PEP, their family members and close associates;
    ii) International Organisation PEP, their family members, and close associates; or (iii) PEP who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with the Regulated Entity present a high risk for ML/TF.

d) The LLP shall also ascertain the source of wealth of the clients by appropriate and reasonable means. (Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns, bank statements, etc.).

e) The LLP should be aware that client relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves. Therefore, the

measures applied for all types of PEPs should also apply to family members or close associates of such PEPs.

f) The LLP shall not automatically treat all individuals who are PEPs, as a high-risk client.

Each PEP should be assessed on risk sensitive basis and the LLP shall determine what risk category is appropriate for such PEPs. In case a PEP is assigned as high risk, the LLP shall undertake the Enhanced Client Due Diligence measures referred under **Clause 9.8.** However, even if a PEP is not assigned a high risk, the LLP shall still undertake the additional client due diligence measures specified in **Clause 9.7. (b)** for PEPs.

g) Source of wealth generally refers to the origin of the client's and beneficial owner's entire body of wealth (i.e., total assets). This relates to how the client and beneficial owner have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the client and beneficial owner would be expected to have. Although the Regulated Entity may not have specific information about assets that are not deposited with or processed by the Regulated Entity, it may be possible to obtain general information from the client, commercial databases or other open sources.

h) Verification of source of wealth can be carried out by various measures including obtaining independent corroborating evidence such as share certificates, publicly available registers of ownership, information and documents such as evidence of title, copies of trust deeds, bank or brokerage account statements, probate documents, audited accounts and financial statements, salary details, tax returns, news items from a reputable source and other similar evidence. For instance:

i) for a legal person, this might be achieved by obtaining its financial or annual reports published on its website or news articles and press releases that reflect its financial situation or the profitability of its business; and
ii) for a natural person, this might include documentary evidence which corroborates answers given to questions on the source of wealth in an application form or client questionnaire. For example, if a natural person attributes the source of his wealth to inheritance, he may be asked to provide a copy of the relevant will or grant of probate. In other cases, a natural person may be asked to provide bank statements, salary statements or tax returns covering number of years to draw up a picture of his source of wealth.

9.8. Enhanced Due Diligence:

a) Where the risks of ML/TF are high, the LLP shall conduct enhanced CDD measures, consistent with the risks identified. The enhanced CDD measures are as follows: -
   i) Obtaining additional information on the client (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of client and beneficial owner.

ii) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the client or, if applicable, of the Beneficial Owner.

iii) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

iv) Obtaining the approval of Senior Management to commence or continue the business relationship.

v) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and,

vi) Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

b) Where applicable, it is required that first payment made by a client in order to open an account with the LLP shall be carried out through a bank account in the client's name with:

i) a Bank;

ii) a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or

iii) a subsidiary of a regulated financial institution referred to in (ii), if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.

c) The Enhanced CDD measures will apply depending upon the risk profile of the client and the extent of its applicability to a client shall be decided on case-to-case basis.

d) Circumstances where a client presents or may present a high probability of ML/TF risk may include, but are not limited to the following:

i) where a client or any beneficial owner of the client is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures; and

ii) where a client or any beneficial owner of the client is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the Regulated Entity for itself or notified to Regulated Entity generally by the Authority or other relevant domestic authorities in India or other foreign regulatory authorities.

e) For establishing an account-based relationship with high-risk clients, the approval may be given by Senior Management or committee of senior managers or an individual member who has been authorised by the Designated Director in this behalf.

f) In cases where a client uses complex legal structures and/or trusts, private investment vehicle, the LLP shall satisfy itself that it is used for a legitimate and genuine purpose.

g) The LLP shall take reasonable measures to examine the source of wealth and source of funds. That is, where the funds for a particular service or transaction will come from (e.g., a

specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the client or, if applicable, of the Beneficial Owner.

h) Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations. In order to ensure that the funds are not proceeds of crime, the LLP should not limit its source of funds inquiry to identifying the other financial institution from which the funds have been transferred, but more importantly, the activity that generated the funds.
The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having been acquired.

i) Examples of appropriate and reasonable means of establishing source of funds are such as proof of dividend payments connected to a shareholding, bank statements, salary payments or bonus certificates, sale proceeds, loan documentation and proof of a transaction which gave rise to the payment into the account.

j) A client should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.

9.9. Simplified Client Due Diligence

a) Where the risks of ML/TF are low, the LLP may conduct simplified CDD measures, which should be commensurate with the low risk factors. Examples of possible measures are:
   i) Verifying the identity of the client and the beneficial owner after the establishment of the business relationship as specified under Clause 5.3.
   ii) Reducing the frequency of client identification updates.
   iii) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
   iv) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.
b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF.
c) Where the LLP applies SCDD measures, it is still required to perform ongoing monitoring of business relations as specified under Clause 9.10.
d) A LLP is not required to identify or verify Beneficial Owners for retail investment funds which are widely held and for investment funds where the investor invests via pension contributions.
e) The LLP may also use other measures to conduct CDD in accordance with the client risks.

9.10. Ongoing client due diligence

While undertaking the ongoing client due diligence, as required under this Policy, the following requirements shall be complied with by a LLP:

i) The LLP shall monitor its business relations with the client on an ongoing basis.

ii) The LLP during the course of business relations with a client, shall observe the conduct of the client's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with LLP's knowledge of the client, its business and risk profile and where appropriate, may seek the source of wealth and source of funds.

iii) The LLP shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose.

iv) The LLP shall make further enquiries into the background and purpose of the transaction specified in sub-clause (iii) above and document its findings so that this information is made available to the relevant authorities, should the need arise.

v) A LLP shall periodically review each client to ensure that the risk rating assigned under **Clause 11.3.** below, is commensurate with the ML/TF risks posed by the client.

vi) Where there are indications that the risks associated with an existing business relation with the client may have increased, the LLP shall request additional information and conduct a review of the client's risk profile in order to determine if additional measures are necessary.

vii) The LLP shall ensure that the Client Due Diligence data, documents and information obtained in respect of clients, natural persons appointed to act on behalf of the clients, related parties of the clients and beneficial owners of the clients, are relevant and kept up-to-date by undertaking the review of adequacy of the existing Client Due Diligence data, documents and information, particularly for clients with high-risk rating.

viii) An essential aspect of ongoing monitoring includes maintaining up-to-date and relevant Client Due Diligence data, documents and information so that the LLP can identify the changes in client's risk profile. The following shall be followed by the LLP: -

(a) for clients who are rated as high risk, the LLP shall obtain updated CDD information (including updated copies of the client's Officially Valid Documents if these have expired), as part of its periodic CDD review, or upon the occurrence of a trigger event as deemed necessary by the LLP, whichever is earlier; and

(b) for all other risk categories of clients, a LLP should obtain updated CDD information upon the occurrence of a trigger event.

ix) A LLP shall undertake a review under sub-clause (v) and (vii) of Clause 5.8, both periodically and at other appropriate times, including when:

(a) the LLP changes its CDD documentation requirements;
(b) an unusual transaction with the client is expected to take place;
(c) there is a material change in the business relationship with the client; or
(d) there is a material change in the nature or ownership of the client.

9.11. Ongoing sanctions screening and Updation

A LLP shall review its clients, their business and transactions against United Nations Security Council (UNSC) sanctions lists and also against any other relevant sanctions list when complying with **Clause 9.1.**

- **Periodic Updation**

A LLP shall adopt a risk-based approach for periodic updation of CDD. The periodicity of updation from the date of opening of the account / last CDD updation for different categories of clients is as follows: -

i) Annually- for high-risk clients;
ii) once in three years- for medium risk client; and,
iii) once in every five years- for low-risk clients.

a) Individual Clients:

(i) No change in CDD information:

In case of no change in the CDD information, a self-declaration from the client in this regard may be obtained through mobile number registered with the LLP or through digital channels (such as online banking / internet banking, e-mail or mobile application of LLP).

(ii) Change in address:

(aa) In case of a change only in the address details of the client, a self-declaration of the new address may be obtained from the client through client's email-id registered with the LLP, client's mobile number registered with the LLP, digital channels (such as online banking internet banking, e-mail or mobile application of the LLP). The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

(bb) Further, a LLP shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address declared by the client at the time of periodic updation.

b) Clients other than Natural Persons:

(i) No change in CDD information:

In case of no change in the CDD information of a client, which is a non-natural person, a self-declaration through email id registered with the LLP, digital channels (such as online banking/ internet banking, mobile application of LLP), a letter duly signed by authorised official and requisite resolutions in this regard shall be obtained from the client. Further, a LLP shall ensure that Beneficial Ownership (BO) information available with them is accurate and upto-date.

(ii) Change in CDD information:

In case of change in CDD information, LLP shall undertake fresh CDD process as is applicable for on boarding a new client which is a non-natural person.

c) Additional measures:

In addition to the above, a LLP shall ensure that:

(i) The KYC documents of the client as per the current CDD standards are available with it. This is applicable even if there is no change in client information but the documents available with the LLP are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the LLP has expired at the time of periodic updation of CDD, LLP shall undertake fresh CDD process equivalent to that applicable for on boarding a new client.

(ii) In case of Indian National, the client's PAN details, if available with the LLP, is verified from the database of the issuing authority at the time of periodic updation of CDD.

(iii) Acknowledgment is provided to the client mentioning the date of receipt of the relevant document(s), including self-declaration from the client, for carrying out periodic updation. Further, the LLP shall ensure that the information / documents obtained from the clients at the time of periodic updation of CDD are promptly updated in its records / database and an intimation, mentioning the date of updation of CDD details, is provided to the client.

(iv) In order to ensure client convenience, a LLP may consider making available the facility of periodic updation of CDD at any of its branch, or in such other facilities.

(v) A LLP shall adopt a risk-based approach with respect to periodic updation of CDD. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the LLP (such as requirement of obtaining recent photograph, requirement of physical presence of the client, requirement of periodic updation of CDD only where account is maintained, a more frequent periodicity of CDD updation than the minimum specified periodicity etc.), shall be clearly specified in its approved internal KYC policy.

(vi) A LLP shall ensure that its internal KYC policy and processes on updation / periodic updation of CDD are transparent and adverse actions against the clients should be avoided, unless warranted by specific regulatory requirements.

9.12 The LLP may rely on a Third Party to perform CDD measures, subject to the following conditions:

(a) The LLP shall obtain records or information of the client due diligence carried out by the third party, immediately;

(b) The LLP shall take adequate steps to satisfy itself that the copies of identification data and other relevant documentation relating to the client due diligence will be made available by the third party upon request, without delay;

(c) The LLP is satisfied that the third party, it intends to rely upon, is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements mentioned under recommendation 10 and 11 of the FATF recommendations and also are in line with the requirements and obligations under the Act;

(d) The third party is not based in a country or jurisdiction assessed as high risk;

(e) No LLP shall rely on a third party to conduct ongoing monitoring of business relations with customers;

(f) No LLP shall rely on a third party specifically precluded by the Authority from relying upon;

(g) The LLP shall document the basis for its satisfaction that the requirements under sub-clause (c) above, have been met;

(h) The LLP is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

(i) Obtaining records or information of the client due diligence under sub-clause (a) above, means obtaining all relevant CDD information, and not just basic information such as name and address.
(j) For the avoidance of doubt, it is clarified that a LLP is not required automatically to obtain the underlying certified documents used by the third party to undertake its CDD. A LLP shall, however, under sub-clause (b) above, ensure that the certified documents are readily available from third party on request.
(k) The LLP shall take appropriate steps to identify, assess and understand the ML/TF risks particular to the countries or jurisdictions that the third party operates in.
(l) Where a particular jurisdiction's laws (such as secrecy or data protection legislation) would prevent a LLP from having access to CDD information upon request without delay, the Regulated Entity should undertake the relevant CDD itself and should not rely on the third party.
(m) If a LLP is not reasonably satisfied that a customer or Beneficial Owner has been identified and verified by a in a manner consistent with these Guidelines, the LLP shall immediately perform the Customer Due Diligence itself with respect to any deficiencies identified.

10. CLIENT'S ACCEPTANCE PROCEDURE

Moneysukh Advisors IFSC LLP has further developed Client acceptance policies and procedures that aim to identify the types of Clients that are likely to pose a higher than the average risk of money laundering or terrorist financing. By establishing such policies and procedures, we are in a better position to apply Client due diligence on a risk sensitive basis depending on the type of Client business relationship or transaction.

10.1. Failure of the RE or Business Facilitator to conduct or complete client due diligence:

In a nutshell, the following safeguards shall be followed while accepting the clients:

- ✓ No account shall be opened in a fictitious / Benami name or on an anonymous basis.
- ✓ Documentation requirement and other information shall be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the laws of the country of the RE or guidelines issued by the FATF from time to time.
- ✓ The LLP shall not open an account where it is unable to apply appropriate Client due diligence measures i.e., the RE is unable to verify the identity and /or obtain documents required as per the risk categorization due to non – cooperation of the Client or non-reliability of the data/information furnished to the RE. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the Client. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the Client explaining the reasons for such a decision;
- ✓ Necessary checks before opening a new account will be performed so as to ensure that the identity of the Client does not match with any person with known criminal background or with sanctioned entities or individual such as individual terrorists or terrorist

organizations or whose name appears in the sanction lists circulated by Financial Regulator of the country or Bodies appointed for this purpose, United Nations Security Council (UNSC), Financial Intelligence Units of the Countries, Ministry of External Affairs etc. or any regulator of the applicable Jurisdiction from time to time. The RE shall prepare a profile for each new Client based on risk categorization, as provided subsequently in this policy. The parameters that will be used for the risk categorization may be manual or mapped into the system used for KYC & AML compliance however the RE shall be responsible for final risk categorization of the Client. The Client profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

- ✓ Factors of risk perception of the client shall be clearly defined having regard to clients' location, nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. These parameters will enable to classify the clients into Unacceptable, Low, Medium and High risk. Clients of special category may, if necessary, be classified even higher. The clients that require higher degree of due diligence and regular update of Risk profile. The RE shall apply the Risk Based Approach for Enhanced or Simplified Client Due Diligence.

- ✓ The adoption of Client acceptance policy and its implementation should not become too restrictive and must not result in denial of Investing facility to members of the general public.

- ✓ Client Due Diligence process will be revisited when there are suspicions of money laundering or financing of terrorism.

10.2. a) In cases where a LLP is unable to conduct or complete the requisite Client Due Diligence for a client in accordance with **Clause 9.1**, it, to the extent relevant, shall: -

i) not open an account or otherwise provide a service;
ii) not carry out a transaction with or for the client;
iii) not otherwise establish a business relationship;
iv) terminate or suspend any existing business relationship with the client;
v) return any monies or assets received from the client; and,
vi) consider whether the failure to conduct or complete Client Due Diligence necessitates the filing of a Suspicious Transaction Report (STR).

b) A LLP is not bound to comply with sub-clauses (a) (i) to (v) above, if it amounts to "tipping off" of the client, or FIU-IND directs the LLP to act otherwise.

c) A LLP while complying under **Clause 10.2** (a), should apply one or more of the measures specified under sub-clauses (i) to (vi) above, as applicable, in the circumstances. In cases where CDD cannot be completed, it is appropriate that the LLP shall not carry out transaction until the completion of pending CDD.

d) Clause 10.1. shall apply to both existing and prospective clients. In case of existing clients, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances.

e) The Risk Based Approach shall be adopted for the Client Due Diligence of the existing clients.

10.3. Business relationship considered Unacceptable Risk:

The LLP shall not establish the business relationship with the client, which is a legal person or legal arrangement, in the following cases: -

(a) where the ownership or control arrangements of the client prevent the LLP from identifying one or more of the client's Beneficial Owners;
(b) where there are anonymous accounts, accounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to the LLP; or
(c) a Shell Financial Institution.
(d) Issuing or dealing in bearer shares or bearer share warrants
(e) Accepting cash payments
(f) Making cash payments (except for petty cash payments to suppliers or staff in accordance with our internal procedures).

Further list of Clients with unacceptable risk shall be classified in the Risk Assessment and Categorization Matrix from time to time. For the above purpose the FATF Public Statement, the reports and guidance notes on KYC/AML issued by the regulator, guidance note circulated by Central bank etc., may also be used in risk assessment.

The aforesaid risk assessment shall be carried out in continuity with the applicability of the AML & KYC procedures and shall be reviewed **annually** by the Designated Partners of the LLP along with the KYC & AML Policy.

11. RISK – BASED APPROACH ("RBA")

It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the legal form, client's location, background, type of business relationship or transaction etc. As such, each of the client's due diligence measures on a risk sensitive basis shall be applied. The basic principle preserved in this approach is that an enhanced client due diligence process shall be adopted for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. The LLP shall adopt Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk to which the LLP or the LLP is exposed, depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc. and document the same. The LLP while adopting RBA shall ensure that:

(i) The RBA is objective and proportionate to the risks;
(ii) The RBA is based on reasonable grounds; and
(iii) The RBA is reviewed and updated at appropriate intervals.

11.1. Risk Assessment

i Risk assessment to be carried out to identify, assess and take effective measures to mitigate money laundering, terrorist financing risk and the risk of bribery or corruption with respect to clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment shall also take into account any country specific information that is circulated by the Government of country, Regulators of country including IFSCA and from the regulators of Foreign Jurisdiction from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions and by FATF.

ii The risk assessment carried out shall also consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The risk assessment shall be done as per the **Risk assessment procedure provided in Annexure – I** and a **Risk Assessment and Categorization Matrix** will be created either manual or embedded in the system used for KYC & AML where the Risk categorization based on the risk-score will be documented and the same shall be updated regularly and made available to competent authorities and self-regulating bodies, as and when required by them.

iii While preparing the internal risk assessment, LLP shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share for the LLP from time to time.

iv The outcome of the risk assessment by the LLP shall be properly documented. The documentation should include the enterprise-wide AML/CFT risk assessment wherever applicable, details of the implementation of the AML/CFT risk management systems and controls as guided by the AML/CFT risk assessment. The LLP shall ensure that the ML/TF risk assessment information are made available to the Authority upon request. The records of documented risk assessment shall be kept as per the requirements of record keeping process specified under these Guidelines.

v The result of the risk assessment shall be used to classify the ML/TF risks as low, medium, and high. The general principle of this classification is to apply enhanced measures in case of high-risk clients and simplified measures in case of low-risk clients.

vi To keep the risk assessments up-to-date, the LLP shall review its risk assessment **at least once every two years** or when a material trigger event occurs, whichever is earlier. The outcome of the exercise shall be put up to the Governing Body or such other committee of the LLP or the LLP to which power in this regard has been delegated.

The LLP has applied Risk Based Approach (RBA) for mitigation and management of the identified risk by established controls and procedures in this regard. Further, the LLP shall monitor the implementation of the controls and enhance them if necessary. The Risk Based Approach shall be based on following controls:

- Client shall be categorised as Unacceptable, Low, Medium, and High risk, based on the assessment and risk perception of the LLP.

- Risk categorisation shall be undertaken based on parameters of risk assessment in terms of the Client's identity, social/ financial status, nature of business activity, information about the clients' business and their locations, manner of making payment for transactions undertaken, bribery and corruption etc. have been defined to enable categorization of Clients into Unacceptable, Low, Medium, and High risk. While considering Client's identity, the ability to confirm identity documents through online or other services offered by issuing authorities or other entities may also be factored in Documentation requirements and other information to be collected in respect of different categories of Clients depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and IFSCA Guidelines as issued by the Regulator.

- Adopting RBA implies the adoption of a risk management process for dealing with Money Laundering (ML) / Terrorist Financing (TF), keeping in mind the magnitude of risk involved in two stages I. Business Risk Assessment and Client Risk Assessment as follows:

11.2. Business Risk Assessment:

Identifying and Assessing business AML risks the LLP shall:

a) take into consideration the nature, size and the complexity of its business activities and take suitable steps to identify its exposure to ML/TF risks;
b) consider the following risk factors, to the extent applicable and relevant, while identifying and assessing the ML/TF risks: -
   i) its type of clients and their activities;
   ii) its business engagement with the countries or geographic areas;
   iii) its products, services, delivery channels and activity profiles;
   iv) the complexity and volume of its transactions;
   v) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and
   vi) the use of new or developing technologies for both new and pre-existing products;
c) based on the assessment and risk identification made at Clause (a) and (b) above, the LLP shall undertake commensurate mitigation measures.

- **New products, business practices and technologies**

a) The LLP shall identify and assess the ML and TF risks that may arise in relation to:

(i) the development of new products, business practices, including new delivery mechanisms; and

(ii) the use of new or developing technologies for both new and pre-existing products.

b) The LLP shall undertake the above risk assessment exercise, prior to the launch or use of such products, practices and technologies and shall take appropriate measures to manage and mitigate the risks.

11.3. Client Risk Assessment

Risks identified while assessing the business risks shall be used for the client risk assessment. The client risk assessment shall be performed while taking into consideration the parameters, or the process as specified below. The outcome of the Client risk assessment shall be used to assign the risk rating of the client as high, medium or low, proportionate to the ML/TF risks.

- **Assessing Client AML risks**

(a) The LLP shall:
(i) undertake a risk-based assessment of every client; and
(ii) assign the client a risk rating proportionate to the ML/TF risks.

(b) The client risk assessment referred to in Clause (a) above, shall be completed prior to undertaking Client Due Diligence for new clients, and also where the LLP otherwise feels necessary, for existing clients.

(c) When undertaking an assessment under Clause (a) (i) above, the LLP shall:

i) identify the client and Beneficial Owner, if any;
ii) obtain information on the purpose and intended nature of the business relationship;
iii) obtain information on, and take into consideration, the nature of the client's business;
iv) take into consideration the nature of the client, its ownership, control structure, and its Beneficial Ownership, wherever applicable;
v) take into consideration the nature of the client's business relationship with the LLP;
vi) take into consideration the client's country of origin, residence, nationality, place of incorporation or place of business;
vii) take into consideration the relevant product, service or transaction; and,
viii) take into consideration the beneficiary of the policy including any Beneficial Owner of such beneficiary, if it is providing the client with a life insurance or other similar policy.

11.4. Transaction Or Delivery Channel Related Risk

Different delivery channels for the acquisition and management of customers and business relationships, as well as for the delivery of products and services, entail different types and levels of risk.
As defined in the IFSCA KYC/AML Guidelines "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-
(a) opening of an account;

(b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether by payment order or other instruments or by electronic or other non-physical means;
(c) the use of a safety deposit box or any other form of safe deposit;
(d) entering into any fiduciary relationship;
(e) any payment made or received, in whole or in part, for any contractual or other legal obligation; and
(f) establishing or creating a legal person or legal arrangement.
When evaluating transaction or delivery channel-related risk, the LLP shall pay particular attention to those channels, whether related to customer acquisition and/or relationship management, or to product or service delivery, which have the potential to favour anonymity; the use of third-party business introducers, intermediaries, agents, or distributors; and the use of third-party payment, or other transaction intermediaries.
Accordingly, while the LLP or the Regulated Entities having business relationships involving product, service or transaction risk the same shall be assessed for ML/TF risks by undertaking the Client Due Diligence Procedure as described in Clause 8 and Clause 9 of this Policy.

Such relationships may involve relationships with following counterparties:

1. Broker
2. Distributor
3. Channel Partner or Service Agents contracted in relation to the Transactions
4. Fund Accountants and Administrators
5. Information Technology Service Providers or Developers
6. Trustees

Such other parties involved in financial transactions including managing of client money, securities or other asset.

11.5. Factors that may indicate high ML/TF risk

When assessing if there is a high risk of ML/TF in a particular situation, a The LLP shall take into account, among other things:

(a) Client risk

i) Whether the clients are from high-risk businesses / activities / sectors, as well as from other sectors as may be identified by it;
ii) Whether the ownership structure of the legal person or arrangement appears unusual or excessively complex;
iii) Whether the business relations are conducted under unusual circumstances (e.g., significant unexplained geographic distance between the LLP and the client);
iv) Whether the companies have nominee shareholders or shares in bearer form;
v) Whether the legal persons or legal arrangements are personal asset holding vehicles; and,
vi) Whether the corporate structure of the client is unusual or excessively complex given the nature of the business.

(b) Country or Geographic risk

i) Whether the countries or jurisdictions the LLP is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its clients (including the LLP's network of correspondent account relationships) have relatively high levels of corruption, organized crime or inadequate AML/CFT measures, as identified by the FATF;
ii) Whether the countries or jurisdictions are identified by any credible body as having significant levels of corruption, terrorism financing or other criminal activities;
iii) Whether the countries or jurisdictions are identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;
iv) Whether the countries or jurisdictions do not have effective systems to counter ML/TF; or not implementing the AML/CFT measures that are consistent with FATF Recommendations;
v) Whether the countries or jurisdictions are subject to sanctions, embargos or similar measures issued by International Organisations or India;
vi) Whether the countries or jurisdictions are funding or supporting the terrorism; and,
vii) Whether countries or jurisdictions have organizations operating within their territory that have been designated by India, other countries or International Organizations as terrorist organizations.

(c) product, service, transaction or delivery channel risk factors

When assessing inherent risks associated with product, service, and transaction types, the LLP must take stock of the lines of business, products and services that are more vulnerable to ML/TF/PF abuse.

The LLP has to assess inherent risks of abuse of the products and services by the customers considering a number of factors such as their ease for holding and transferring value or their complexity and transparency. The Following factors include:

i) Whether the service involves private banking;
ii) Whether the product, service or transaction is one that might favour anonymity;
iii) Whether the situation involves non-face-to-face business relationships or transactions, without adequate safeguards;
iv) Whether the payments received are from unknown or unassociated third parties;
v) Whether the services offered are in relation to nominee directors, nominee shareholders or the formation of companies in another country; and
vi) Whether there are anonymous transactions or any transaction which involves frequent payments, received from unknown or unassociated third parties.

When assessing the risk factors, the LLP shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a high risk of ML/TF in a particular situation.

11.6. Factors that may indicate low ML/TF risks

When assessing if there is a low risk of ML/TF in a particular situation, a LLP shall take into account, among other things:

(a) client risk factors, including whether the client is:

i) a Government entity;
ii) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
iii) regulated financial institution incorporated or established outside India that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.
iv) a subsidiary of a regulated financial institution referred to in sub-clause (iii) above, if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML standards as that of its Parent entity;
v) a public body or a publicly owned enterprise;
vi) a resident established or registered in a geographical area of low risk;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

i) a Contract of Insurance that is non-life insurance;
ii) a Contract of Insurance that is a life insurance product with no investment return or redemption or surrender value;
iii) an insurance policy for a pension scheme that does not provide for an early surrender option and cannot be used as collateral;
iv) a Contract of Insurance which is a reinsurance contract that is ceded by an insurer which is a regulated financial institution;
v) a pension, superannuation or similar scheme that satisfies the following conditions:
(aa) the scheme provides retirement benefits to employees;
(bb) contributions to the scheme are made by way of deductions from wages; and
(cc) the scheme rules do not permit the assignment of a member's interest.
vi) a product where the ML/TF risks are adequately managed by other factors such as transaction limits or transparency of ownership; and
vii) financial products or services that provide appropriately defined and limited services to certain types of clients (e.g., to increase client access for financial inclusion purposes).

When assessing the risk factors, the LLP shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a low risk of ML/TF in a particular situation.

12. BUSINESS FACILITATOR:

The undertaking of verification of Identity, CIP and CDD procedures under this policy and maintaining the records is outsourced to the ___ Moneysukh Advisors IFSC LLP _____as a business facilitator. The rationale for such outsourcing is that the business facilitator, has adequate infrastructure and experience to perform the CDD process on behalf of the LLP.

The LLP and business facilitator shall entered in a written agreement in respect of the performance of the AML Obligations.

The LLP remains ultimately responsible for the performance of AML activities on its behalf as the LLP has majority powers to undertake business with Clients. The business facilitator shall undertake all necessary CDD measures and will grant access to CDD information without delay upon request by the LLP.

The Designated Partners of the LLP shall monitor the outsourcing (i.e. amongst others the performance and adequacy of the services provided by the business facilitator r in this respect) at least once per annum.

a) the LLP shall obtain records or information of the client due diligence carried out by the business facilitator.
b) The LLP shall take adequate steps to satisfy itself that the copies of identification data and other relevant documentation relating to the client due diligence will be made available by the business facilitator upon request, without delay.
c) The LLP is satisfied that the business facilitator r, is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements mentioned under recommendation 10 and 11 of the FATF recommendations and also are in line with the requirements and obligations mandated by IFSCA;

13. RECORD KEEPING & RETENTION OF RECORDS

The following steps shall be taken regarding maintenance, preservation and reporting of Client account information, with reference to provisions of AML/CFT and its Rules. The LLP will:

(a) Maintain all necessary records for at least six-years from the date on which business relationship has ended or transaction is completed. The LLP shall maintain following records:

1. a copy of all documents and information obtained in undertaking initial and ongoing Client Due Diligence;
2. records of client business relationships (both original and certified copies), which include:
   i correspondence of business and other information relating to a client's account
   ii adequate records of transactions to enable standalone transactions to be reconstructed; and
   iii internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;
3. All relevant details of transactions and persons involving Money Laundering and Terror Financing notified by an Employee, in the ordinary course of employment.
4. Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis
5. any relevant communications, if made with the FIU
6. all risk assessment documents as specified in sub-clause (d) of this Clause.
7. any other matter that the LLP may be expressly required to record and maintain, under Guidelines.

(b) Where the date of Business Relationship ended with client remains unclear, the date of the completion of the last transaction shall be considered.

(c) make available the identification records and transaction data to the competent authorities upon request immediately.

(d) The LLP shall also keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including :
   1. Business risk assessment undertaken
   2. Analysis of using Business risk assessment for the purpose of Client Risk Assessment
   3. Risk assessment of its client undertaken,
   4. Determination of risk rating

(e) The records may be kept in Electronic Form in such a way that records are readily accessible and are promptly made available to the authority upon request.

(f) The system for proper maintenance and preservation of records shall fulfil the conditions mentioned below:
   1. Data to be retrieved easily and quickly whenever required or when demanded
   2. Allows the Authority is able to assess the LLP's compliance with the applicable laws
   3. Allows identification of a client or third party
   4. Permits reconstruction of any transaction which was processed by or through the LLP on behalf of a client or other third party.

14. MONITORING OF TRANSACTIONS

Regular monitoring of transactions is an essential element of effective AML procedures. The LLP can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the client so that they have the means of identifying transactions that fall outside the regular pattern of activity.

Special attention shall be paid to all complex unusually large transactions / patterns which appear to have no economic purpose.

The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to Regulator other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of six years from the date of transaction between the client and the LLP.

Further, the LLP shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.
A suspicious activity will often be one which is inconsistent with a Client's known, legitimate business or personal activities or with the normal business for that type of LLP and which may prompt a suspicion of money laundering or Terror Financing. Typically, suspicious activities are those that appear to have no sound commercial reason, or which do not constitute the most logical, convenient, or secure way to do business. Unusual transactions can be discovered by anyone in the acceptance procedure (even if the Client is not accepted (yet)) as well as during maintaining the business relationship.

Further, appropriate steps shall be taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions.

A list of circumstances which may be in the nature of suspicious transactions and act as a "Red Flag" includes:

a) Clients from unacceptable risk category
b) Clients whose identity verification seems difficult or clients that appear not to cooperate
c) Clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
d) Change of bank account at the redemption of Investment proceeds
e) Frequent Closures or changes of Bank accounts of the Client
f) Change in the jurisdiction of the Bank account of the Client
g) Clients' location or the Bank account of the Client is changed to high risk jurisdictions;
h) Substantial increases in investment above the Net-Worth without apparent cause;
i) Attempted transfer of investment proceeds to apparently unrelated third parties;
j) Unusual transactions by Special Category Client under EDD
k) Client's businesses reported to be in the nature of export- import of small items or engagements with terrorist countries
l) complex, unusual or large transactions that have no apparent economic or lawful purpose.

Further, this list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances.
If an employee, in his ordinary course of his employment, either knows, suspects or has reasonable ground for knowing or suspecting of any suspicious transaction shall be immediately notified to the Principal Officer or Senior Reporting Officer or any other designated officer within the LLP. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. Employees may ask client relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.

However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the client and this may include:

a) the client's usual occupation, business or principal activity;
b) the client's transaction history;
c) the client's risk profile;
d) the client's income level;
e) the clients source of income as stated during account opening or initial engagement;
f) reasons for the transactions as provided by the client;
g) the "relationship" of the client with the sender or beneficiary of funds
h) the frequency of transactions;
i) the size and complexity of the transaction;
j) the identity or location of any other person(s) involved in the transaction;
k) the usual or typical financial, business or operational practices or behaviour of clients in the similar occupation or business category; and

l) the availability of identification documents and other documentation.
m) If the LLP finds that the Client's Profile has changed, it shall update the Client's Profile.

The Employees shall evaluate the suspicious indicators, information solicited from the client through questions asked and known information about the client to determine if there are reasonable grounds to suspect that the transaction(s) is related to the commission of a ML/ TF or any other serious offence. If it is concluded that there are reasonable grounds to suspect that the transaction(s)or attempted transaction(s) is linked to a Money Laundering / Terror Financing or any other serious offence, after reporting the same to the Principal Officer with clearly it should be reported to FIU-IND by completing and submitting a Suspicious Transaction Report. Also in exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

15. REPORTING OF SUSPICIOUS TRANSACTIONS TO FIU-IND

i) A LLP shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), the required information referred to in rule-3 of the Rules and in accordance with the terms of rule-7 thereof.
ii) The reporting formats and comprehensive reporting format guide prescribed or released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Regulated Entities in the preparation of prescribed reports shall be taken note of.
iii) Suspicious Transaction Reports (STR) which FIU-IND has placed on its website, shall be made use of by Regulated Entities which are yet to install/adopt suitable technological tools for extracting STR from their live transaction data.
iv) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation.
v) In terms of the Rules, the Regulated Entities are mandated to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Tower-2,
Jeevan Bharati Building,
Connaught Place,
New Delhi-110001,
Telephone: 91-11-23314429, 23314459
Website: http://fiuindia.gov.in

The Regulated Entities shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND.

vi) (a) Further, in terms of Rules, the Regulated Entities shall inter-alia adhere to the following:
(i) The Suspicious Transaction Report (STR) shall be submitted promptly on arriving at a conclusion that any transaction or a series of transactions that are integrally connected, are

of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

(ii) The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

(iii) The Principal Officer shall be responsible for timely submission of STR and NTR to FIU-IND;

(iv) Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND.

4) In terms of the Rules, the Regulated Entities are mandated to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the above mention address.

vii) The requirement to report any suspicious transaction applies to all types of transaction. There is no minimum monetary threshold amount for reporting suspicious transactions. Thus, a transaction considered suspicious should be reported to the FIU-IND regardless of the currency or amount of the transaction.

viii) If the LLP or the LLP is not able to obtain satisfactory evidence of a client's identity, the LLP should not proceed further with the transaction unless directed in writing to do so by the FIU-IND.

ix) If the LLP or the LLP considers the reasons for the client's failure or refusal to produce adequate identification documentations as unreasonable or suspicious, it shall report the attempted transaction to the FIU-IND as a suspicious transaction.

x) The Regulated Entities and its employees or agents shall not disclose to any person (including the client).

xi) Disclosure of information on suspicious transactions is only allowed for exceptional circumstances or regulatory purposes.

16. COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS:

1) The LLP shall ensure that it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto and which are approved by and periodically circulated by the United Nations Security Council (UNSC).The details of the two lists are as under:

a. The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al- Qaida Sanctions List is available at:

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

b. The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl

2) Details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, which is available at: https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf

3) In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

4) The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly followed and compliance with the Order shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

5) FATF Statements circulated from time to time, and publicly available information for identifying countries which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

6) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or emanating in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in the FATF statements.

7) The process referred to in (5) and (6) above, do not preclude Regulated Entities from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

8) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations as aforesaid shall be examined, and written findings, together with all documents, shall be retained and be made available to the Authority and other relevant authorities, on request.

9) A LLP shall maintain secrecy regarding the client information that arises out of the contractual relationship between it and the client. All the information shall be treated as confidential and shall not be divulged without the express consent of the client.

10) While considering the requests for data/information from Government and other agencies, a LLP shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy.

11) The LLP shall provide the information sought where:
   a. disclosure is under compulsion of law
   b. there is a duty to the public to disclose
   c. the interest of LLP requires disclosure
   d. the disclosure is made with the express or implied consent of the client

12) Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

   Under FATCA and CRS, the LLP shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether it is a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

   a. Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link: https://incometaxindiaefiling.gov.in/ post login > My Account --> Register as Reporting Financial Institution;
   b. Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.
   c. The LLP shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at https://fedai.org.in/ for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.
   d. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
   e. Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
   f. Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
   g. Ensure compliance with updated instructions/ rules/ guidance notes/ Press Releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. A LLP shall also take note of updated Guidance Note on FATCA and CRS and a press release on 'Closure of Financial Accounts' under Rule 114H.

13) Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR)

   a. In terms of provision of rule 9(1A) of Rules, the LLP shall capture client's KYC records and upload on CKYCR within 10 days of commencement of an account-based relationship with the client in the form and manner as prescribed under Central KYC Registry Operating Guidelines 2016, released by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) and shall ensure that:

      i. the KYC records to be uploaded are as per KYC Template released by CERSAI

ii. Once KYC Identifier is generated by CKYCR, the same is communicated to the Client
iii. It has performed the last KYC verification or has sent updated information in respect of a Client to CKYCR

b. Where a client, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the LLP with an explicit consent to download records from CKYCR, such LLP shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the client 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 client as existing in the records of CKYCR
ii. the current address of the client is required to be verified; and
iii. the LLP considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

17. PAYMENT TRANSPARENCY STANDARDS

17.1 Correspondent Banking

The LLP shall have a policy approved by its Governing Body, or by a committee headed by the Chairman/CEO/MD/Director/designated partner to lay down parameters for approving correspondent banking relationships subject to the following conditions namely:-

1. Assessment of the suitability of the respondent bank by taking the following steps:
    a. gather adequate information about the respondent bank to fully understand the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates
    b. determine from the available sources, the reputation of the respondent bank and the quality of supervision over it, including whether it has been the subjected to any ML/TF investigation or regulatory action
    c. assess the respondent bank's AML/CFT controls and ascertain whether they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates;
2. the responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
3. obtain approval from the Senior Management before providing correspondent banking or similar services to a respondent bank.
4. in the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the clients having direct access to the accounts and is undertaking ongoing 'due diligence' on them.
5. The correspondent bank shall ensure that the respondent bank is able to provide the relevant client identification data immediately on request.
6. Correspondent relationship shall not be entered into with a bank which is a Shell Financial Institution.
7. It shall be ensured that the correspondent banks do not permit their accounts to be used by bank which is a Shell Financial Institution.

8. It shall be cautious with respondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
9. (It shall be ensured that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

17.2 Wire Transfers

- This Clause shall apply to a LLP Entity when it sends funds by wire transfer or when it receives funds (including serial payments and cover payments) by wire transfer on the account of the wire transfer originator or the wire transfer beneficiary, but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary, respectively
- The LLP shall monitor payment messages to and from high-risk countries or jurisdictions, as well as transactions with high risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.
- Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or a terrorist entity, the LLP shall block, reject or freeze assets of these terrorists or terrorist entities immediately.
- Where there are positive hits arising from name screening checks, they should be escalated to the Principal Officer. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and be documented.
- A LLP shall not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another LLP in the payment process.
- The process for Wire transfer shall not cover the below mentioned transactions when a credit, charge, debit or prepaid card is used as a payment system to effect a person-to-person wire transfer. In such a case, the necessary information should be included in the message for such transactions.:
  a. any transfer that flows from a transaction carried out using a credit, charge, debit or prepaid card for the purchase of goods or services, so long as the credit, charge, debit or prepaid card number accompanies all transfers flowing from the transaction.
  b. transfers and settlements between the entities, where both the originator and the beneficiary are Regulated Entities acting on their own behalf.

18. AUDIT, EMPLOYEE TRAINING AND AWARENESS:

18.1 Audit:

The LLP shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the LLP's internal policies, procedures and controls, in compliance with regulatory requirements and these Guidelines. The LLP's AML/CFT framework should be subjected to **annual** audits. Such audits should be performed not just on

individual business functions but also on a LLP or Regulated Entity-wide basis. Auditors should assess the effectiveness of measures taken to prevent Money Laundering/Terror Financing. This would inter-alia include ―

a. Determining the adequacy of the LLP's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;
b. Reviewing the content and frequency of AML/CFT training programmes, and the extent of employee's, officer's and representative's compliance with established AML/CFT policies and procedures; and
c. Assessing whether instances of non-compliance are reported to Senior Management on a timely basis. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the LLP's business.

18.2 Training and Awareness:

The LLP shall :

1. Provide AML/CFT training to all relevant employees, **Annually** and on **On-Going Basis** will performing the activities covered under this Policy.
2. Ensure that its AML/CFT training enables its employees to:
   i. comprehend the applicable laws relating to ML/TF, including the Act and Rules
   ii. understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto
   iii. recognise and deal with transactions and other activities which may be related to ML/TF
   iv. comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;
   v. have knowledge of the prevailing techniques, methods and trends in ML/TF, relevant to the business of the LLP;
   vi. understand their roles and responsibilities in combating ML/TF, including the identity and duties of the LLP's Principal Officer and deputy, where applicable; and,
   vii. understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in the Risk Assessment Procedure.

3. ensure that its AML/CFT training:
   i. is relevant and tailored to the LLP's activities, including its products, services, clients, distribution channels, business partners, level and nature of its transactions; and
   ii. identifies and indicates the different levels of ML/TF risk and vulnerabilities associated with the matters in sub-clause (c)(i) above.

4. All the new relevant employees of the LLP should be given appropriate AML/CFT training as soon as reasonably practicable after commencing employment with the LLP or the Regulated Entity. Such training may not necessarily be formal and may include any medium which is considered appropriate.

5. A relevant employee may include a member of the Senior Management or operational staff, any employee with client contact or who handles or may handle client monies or assets, and any other employee who might otherwise encounter ML/TF in the business context.

18.3 Employees Hiring:

The LLP will have adequate screening procedures in place to ensure high standards when hiring employees. The key position shall be identified having regard to the risk of money laundering and terrorist financing. LLP shall further ensure that the employees taking up such key positions are suitable and competent to perform their duties. Further, KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse LLP's infrastructure.

AML/CFT policies, standards and procedures are effectively communicated, and the foundation a 'tone from the top' message from Senior Management and apply to persons at all levels of the LLP. Training and/or communications should also be provided to employees in this regard upon joining.

The HR Department is instructed to verify the identity, cross check all the references, family background and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting.

The department should obtain the following documents:

1. Photographs
2. Proof of address
3. Identity proof
4. Proof of Educational Qualification
5. Proof of Bank Account Details

LLP shall have an ongoing employee training programme for the applicable employees engaged in the function of Client On-Boarding so that the members of the staff are adequately trained in KYC and AML procedures. Training requirements shall have specific focuses for frontline staff, back-office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

19. Anti-Bribery and Corruption (ABC) Compliance:

The LLP must combat the corruption in the form of bribery, which is commonly described as involving the offer, promise, request, acceptance, or transfer of anything of value either directly or indirectly to or by an individual, to improperly induce, influence, or reward the performance of a function or an activity.

Bribery risks are not limited to cash payments and may arise from an offer or transfer of anything of value. Accordingly, the LLP hereunder establishes the risk-based controls to mitigate risks associated with the following activities:

- Gifts and Business Hospitality
- Employment and Work Experience
- Charitable Giving
- Political Contributions

- Marketing Sponsorships

Need for the ABC Compliance:

Bribery risks generally are greater for Financial Institutions when pursuing business opportunities from, or providing benefits to, a government or wholesale client entity (wholesale client) rather than a client in his/her individual capacity (e.g., a private wealth client).

Public Officials whether domestic or foreign, as well as their representatives/agents, present higher corruption risks for companies seeking to obtain or retain government business or to obtain or influence government action (e.g., legislative action, regulatory approvals or licensing).

The LLP defines Public Officials as individuals at any rank or level at the following types of organisations:

- National, regional, local or municipal governmental bodies (e.g., executive, legislative, judiciary)
- State-owned or state-controlled companies. Generally, an entity would be deemed state-controlled where a government body has at least one of the following attributes:

More than 50% ownership or Voting control or Board control or other indicia of control.

- Central banks
- Sovereign wealth funds
- International organisations, development banks and public health agencies (e.g., the United Nations, EU, World Bank or IMF), as well as mixed private-public entities
- Royal families
- Political parties, party officials, and candidates for any level of political office.

The ABC compliance shall have following standards:

A. Compliance Programme Guidance:

- Prohibition of falsifying or concealing any books, records or accounts that relate to the business of the firm, its clients, suppliers or other business partners.
- Prohibition of the promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly through third parties, if improperly intended to influence action or obtain an advantage.
- Zero tolerance for bribery and similarly prohibit facilitation payments.
- There is a potential bribery and corruption risks that can arise in departments such as Corporate Affairs, Marketing, Sponsorships, Facilities, Business Development, Real Estate and Procurement, particularly given the close interaction with external vendors and service providers. The same are prohibited and any act of corruption or bribery reported under this policy shall be viewed strictly and be treated as provided under this policy.
- Certain temporary staff, outsourced service providers, contractors and other personnel, by virtue of their role, shall also be in scope of ABC Compliance.

B. Reporting and Investigation of Alleged Misconduct

The LLP puts in place the following process to receive, investigate, resolve and document reports of alleged misconduct, including bribery and corruption:

The reporting mechanisms that are available to all employees and, potentially, external parties, which could allow for anonymous reporting, where legally permissible includes

reporting to the Compliance Officer. Further, the LLP shall ensure and publicise that employees who make good faith reports of potential misconduct will not be subject to retaliation.

The LLP ensures process for persons who are responsible for undertaking investigations into bona fide allegations of misconduct. There shall be appropriate confidentiality throughout the process (i.e., a need-to-know-basis) and compliance with applicable laws or regulations. In some situations, the LLP may retain outside counsel or accounting resources to assist in conducting the investigation.

Appropriate disciplinary measures should be taken when an investigation confirms a violation of anti-corruption laws or the Policy. The LLP shall also take steps to remedy the individual harm of such activity and, if required, reasonable steps to mitigate its re-occurrence in the future shall be taken.

The LLP has covered the Bribery risk in the development of controls relating to the procurement of goods and services. In particular, the selection of third-party service providers, as well as restrictions on the receipt of anything of value from such third parties by employees involved in the selection process. On-boarding procedures should also include bribery-related questions or guidance in general procurement questionnaires to help identify those circumstances under which a third-party may present increased bribery risks. Increased risks may require enhanced due diligence (EDD), oversight and appropriate contractual protections, when entering into such engagements.

Certain third parties may pose higher risk for bribery. In particular, these include third parties who act for or on behalf of Financial Institutions to: 1) find, introduce, obtain or maintain business or any other commercial advantage or 2) obtain government approvals or action (collectively herein "Intermediaries").

The LLP may suffer substantial legal liability and reputational risks from the third parties and as a result, it should be appropriately managed throughout the lifecycle of the engagement. As repeatedly identified in enforcement actions, payments to Intermediaries have been used to make and conceal bribes to Public Officials or wholesale clients.

As a result of these inherent risks, the LLP shall: 1) take an expansive view of which third parties should be considered as Intermediaries and 2) risk assess potential engagements to inform the appropriate level of due diligence, approvals and monitoring.

Depending on the assessment subsequent due diligence may include:

- Media searches for negative news related to bribery and corruption. Higher-risk Intermediaries may warrant local language media searches.
- Court record searches for criminal or civil actions related to bribery and corruption.
- If the Intermediary is regulated, checks of public databases for censures, penalties and verification of valid license status.

20. Investors Education

As the implementation of KYC and AML procedures being sensitive subject and requires us to demand and collect certain information from investors which may be of personal in nature or has hitherto never been called for, which information include documents evidencing source of funds/income tax returns/bank records etc. and can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need for us to sensitize the clients about these requirements, as the ones emanating from AML and CFT framework. We shall circulate the AML/CFT Circulars and other specific literature/pamphlets etc. so as to educate the client of the objectives of the AML/CFT program. The same shall also be emphasized on, in the Investor Awareness Programs as may be conducted by us at from time of time.

(Annexures to follow)

Annexure – I

Client Risk Assessment Procedure

1. Collection of Client KYC documents from Client by the LLP or the Business Facilitator, as per the KYC Checklist for different types of Clients as the case may be along with Account Opening Form.
2. Client KYC Screening on the KYC Check Software and Manual screening.
3. Listing the disclosures made by Investor in Source of Funds/Wealth Declaration.
4. Aggregating all the information collected in the Account Opening Form and separately upon further inquiries.
5. Risk Rating of the client based on parameters provided in the Risk Assessment and Categorization Matrix maintained by the LLP for each Client.
6. Risk categorization of the Client. A risk classification will be provided in respect of each Client based on the risk matrix designed by the LLP. The risk categorization will determine whether a Client will be categorized into low risk, medium risk, or high-risk category.

   (a) High Risk - Any Client who scores a total risk rating which is high based on the below categories will be classified as a high-risk investor. Over and above the standard CDD required under this policy, enhanced due diligence will be carried out. Acceptance of such clients will also have to be approved by the Designated Partners of the LLP.

   (b) Medium Risk : Standard CDD will be carried out with certain requirements of Enhanced Due Diligence based on specific requirements.

   (c) Low Risk: Standard CDD will be carried out except where the LLP assesses that simplified due diligence measures may be applied.

****

Annexure-II

(refer Clause 8.4)

DIGITAL KYC PROCESS FOR INDIAN NATIONALS

For undertaking CDD of Indian nationals, the Regulated Entities 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: -

(i) the customer decides to submit his Aadhaar number voluntarily to a bank or any Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(bb) 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 the customer's identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof, 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 Regulated Entity:

Provided that where the customer has submitted,

(i) Aadhaar number under Clause (a) above, to a bank or a Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act, such bank or Regulated Entity shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Regulated Entity.

(ii) proof of possession of Aadhaar under sub-clause (aa) above, where offline verification can be carried out, the Regulated Entity shall carry out offline verification.

(iii) an equivalent e-document of any OVD, the Regulated Entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a live photo as specified under digital KYC Process as specified under Annexure I of Rules.

(iv) any OVD or proof of possession of Aadhaar number under (a)(i)(bb) above where offline verification cannot be carried out, the Regulated Entity shall carry out verification through digital KYC Process as specified under Annexure I of Rules.

Provided that for a period not beyond such date as may be notified by the Government for a class of Regulated Entities, instead of carrying out digital KYC, the Regulated Entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Explanation I: LLP shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

Explanation II: Biometric based e-KYC authentication can be done by authorised official of the Regulated Entity/business facilitators.

Explanation III: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.