POLICY AND PROCEDURE IN COMPLIANCE WITH THE REQUIREMENTS OF

THE PREVENTION OF MONEY- LAUNDERING ACT, 2002

ADOPTED BY

SYSTEMATIX CORPORATE SERVICES LIMITED

1. INTRODUCTION

The Prevention of Money Laundering Act, 2002 (“PMLA”) and the Prevention of Money-Laundering Rules, 2005 (“PML Rules”) as amended from time to time and notified by the Government of India, mandate every reporting entity to adhere to maintain records and report such transactions as prescribed therein to the relevant authorities. The PML Rules, inter alia, empower regulators to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by the regulator.

This policy stipulates the essential principles for combating Money Laundering (ML) and Terrorist Financing (TF) and provides detailed procedures and obligations to be followed and complied with by the company with respect to the following transactions:

1. Managing of Public Issue of Securities;
2. Underwriting connected with the aforesaid Public Issue Management Business;
3. Managing/advising on International Offerings of Debt/Equity i.e. GDR, ADR, bonds and other instruments;
4. Private Placement of Securities;
5. Primary or Satellite dealership of Government Securities;
6. Corporate Advisory Services related to Securities Market e.g. take-overs, acquisitions, Disinvestment;
7. Advisory services for Projects;
8. Syndication of rupee term loans;
9. International Financial Advisory Services.

It is emphasized that the registered intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

As per the provisions of the Act the Company shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under PMLA. Such transactions include:

1. All cash transactions of the value of more than Rs. 10 Lakhs (Rupees Ten Lakhs only) or its equivalent in foreign currency.

2. All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

3. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as d-mat account, security account maintained by the Company.

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.

It is also to be noted that there is NO cash transactions with the Clients of the Company as the Company is primarily into Merchant Banking Activities.

2. POLICE SCOPE AND APPLICABILITY

(a) All clients engaging the Merchant Banker for any permissible activity.

(b) All counterparties, vendors, and intermediaries associated with transactions.

(c) All beneficial owners, promoters, key management personnel, and Ultimate Beneficial Owners (UBOs);

(d) All jurisdictions in which the Merchant Banker operates or conducts transactions

3. IMPORTANT DEFINITIONS

3.1. **"Customer" or "Client"** includes (a) a person who is engaged in or proposes to engage in a financial transaction or activity with a reporting entity (b) a person on whose behalf the person who engaged in the transaction or activity, is acting;

3.2. **"Money- Laundering"** includes the process by which a person 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 proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property;

3.3. **Politically Exposed Persons" or "PEP"** includes individuals who are or have been entrusted with prominent public functions in a domestic or a foreign country, e.g., Heads of States or of Governments, politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. It also includes the Former PEP, family members or close relatives of PEPs;

3.4. **"Negative List"** includes but is not limited to:

Sr.no.	Negative List	Source(Website name and Link)
1.	List of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions	United Nation Security council (https://www.un.org/securitycouncil/content/un-sc-consolidated-list)
3.	List of Entities/Individuals in the Financial Intelligence Unit – India (FIU-IND) list	FIU- India (https://fiuindia.gov.in/)
4.	Entities/Individuals from Black listed countries as per Financial Action Task Force	FATF (https://fiuindia.gov.in/)

	website.	
5.	List of Individuals/Entities as per section 12A of the Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005	FIU- India(https://fiuindia.gov.in/)

3.5. **“PMLA Act”** means the Prevention of Money-Laundering Act, 2002;

3.6. **“PMLA Rules”** means the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and amendments thereto;

3.7. **“Principal Officer”** means the Principal Officer designated by the respective Entity under the PMLA Act;

3.8. **“Reporting Entity”** means a banking company, financial institution, intermediary or a person carrying on a designated business or profession as defined under PMLA Act;

3.9. **“Clients of Special Category (CSC)”**

a. Non -resident clients;
b. High net-worth clients;
c. Trust, Charities, Non-Governmental Organizations (NGOs)and organizations receiving donations;
d. Companies having close family shareholdings or beneficial ownership;
e. Politically Exposed Persons
f. Clients in high risk countries
g. Non face to face clients
h. Clients with dubious reputation as per public information available etc

The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

Words and expressions used but not defined herein shall have the same meanings as ascribed to them under the AML laws.

4. APPOINTMENT OF OFFICERS FOR ENSURING COMPLIANCE WITH PROVISIONS OF PMLA

4.1. <u>Appointment of a Principal Officer:</u> To ensure that the Company properly discharges its legal obligations to report suspicious transactions to the authorities, the Company shall appoint a Principal Officer. The Principal Officer shall act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of ‘Principal Officer’ including any changes therein shall also be intimated to the Office of the Director-FIU-IND.

4.2. Appointment of a Designated Director: The Company, in addition to the Principal Officer shall also designate Managing Director or a Whole-Time Director and in the absence of same, any director of company authorized by the Board of Directors; as a 'Designated Director', in terms of the PML Rules to ensure overall compliance with the obligations imposed under chapter IV of the PMLA and PML Rules. The Company shall communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU – IND.

5. POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

5.1. Obligation to establish policies and procedures

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing.

The Company shall:

a. ensure that the content of this policy are understood by all staff members;
b. regularly review the policy and procedures on the prevention of ML and TF to ensure their effectiveness;
c. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
d. undertake client due diligence measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction.
e. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities.
f. develop staff members' awareness and vigilance to guard against ML and TF.

5.2. Policies and Procedure to combat ML shall cover :

a. Communication of policies relating to prevention of ML and TF to all management and relevant staff that handle merchant banking transactions, money and client records etc. whether in branches, departments or subsidiaries;
b. Client acceptance policy and client due diligence measures, including requirements for proper identification.
c. Maintenance of records.
d. Compliance with relevant statutory and regulatory requirements.
e. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
f. Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard; and,
g. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

6. WRITTEN ANTI MONEY LAUNDERING PROCEDURES

The company is required to adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia the following four specific parameters which are related to the overall 'Client Due Diligence Process':

a. Policy for acceptance of clients.
b. Procedure for identifying the clients.
c. Risk Management.
d. Monitoring of Transactions.

7. CLIENT DUE DILIGENCE ("CDD"): -

7.1. Elements of Client Due Diligence Policy

The objective is to ensure that:

a. The Company obtains sufficient information about the client in order to identify who is the actual beneficial owner or on whose behalf transaction is conducted.
b. Before establishing any business relationship, the company must obtain and verify the following information from all clients

   i. **In case of Company:** Charter documents, PAN, Income Tax and GST returns, Audited Financials for last 3 years.

   ii. **In case of Individual:** Aadhar, PAN, Passport, Driving Licence, Income Tax returns

c. Verify the customer's identity using reliable, independent source, document, data or information.
d. Conduct ongoing due diligence and continuous scrutiny of the client until completion of the transaction to ensure that all transactions conducted are consistent with the client's background, financial status, activities, and risk profile..

Though it is not possible to know all details and exact details of the client's background and financial status, it should be our Endeavour to make a genuine attempt towards achieving this. This will be done in two ways:

7.2. Client Acceptance Policy:

The Client Acceptance Policy lays down explicit criteria for acceptance of clients. The Clients Acceptance Policy must ensure the following aspects of client relationship with the Company:

1. No customer is boarded or entered into an agreement in anonymous or fictitious/ benami name(s)
2. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk.
3. Necessary checks including against the negative list before on-boarding a Client or entering into an agreement or engagement are undertaken, so as to ensure that the identity of the client does not match with any person with commonly established criminal background or reputation or is not banned in any other manner whether in terms of criminal or civil proceedings by any

enforcement agency worldwide including regulators and tax authorities or with banned entities such as individual terrorists or terrorist organizations;

4. Company officials must be satisfied as regards KYC due diligence, as defined under this policy, of the customer.
5. The registered intermediaries shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC).
6. No transaction is undertaken without following the KYC due diligence procedure.

7.3. <u>Client identification procedure (CIP):-</u>

To follow the Client Identification procedure we need to follow following factors:

The 'Know your Client'(KYC) policy should clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

The client should be identified by using reliable sources including documents / information which is provided by the clients at the time of establishing the intermediary – client relationship. We should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship. Appropriate risk management systems to be put in place to determine whether the client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic database of reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

The Company is required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines. Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority of the company.

Further, we should also maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided. The underlying principle should be to follow the principles enshrined in the PML Act, 2002 as well as the SEBI Act, 1992 so that the intermediary is aware of the clients on whose behalf it is dealing.

7.4. <u>Reliance on third party for carrying out Client Due Diligence (CDD)</u>

The Company may rely on a third party for the purpose of –

a) identification and verification of the identity of a client and
b) Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party

shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PMLA.

c) Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. In terms of Rule 9(2) of PML Rules:
   i. The Company shall immediately obtain necessary information of such client due diligence carried out by the third party;
   ii. The Company shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
   iii. The Company shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PMLA Act and PML Rules.
   iv. The third party is not based in a country or jurisdiction assessed as high risk;
   v. The Company shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

8. RISK MANAGEMENT

8.1. Risk-based Approach

a) The company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk. The Company shall monitor the implementation of the controls and enhance them if necessary.

b) The company shall categorize clients in higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction, product, service, or geographic location. The company shall apply each of the client due diligence measures on a risk sensitive basis. The company shall adopt enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that company shall obtain will depend on the risk category of a particular client.

c) Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the client does not in fact pose a low risk.

8.2. Risk Assessment

a) The company shall carry out risk assessment to identify, assess and take effective measures to mitigate its ML/TF risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

b) The risk assessment carried out shall 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 assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

c) The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI 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.

9. TRANSACTION MONITORING:

9.1. <u>Identification / Monitoring of the suspicious Transactions</u>

a. The company shall ensure a record of the transactions is preserved and maintained and that transactions of a suspicious nature or any other transactions notified under PMLA Act are reported to FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the company

10.SUSPICIOUS TRANSACTION MONITORING AND REPORTING:

The company shall put in place systems to identify transactions on the basis of defined parameters and shall generate alerts for further analysis and reporting of suspicious transactions to FIU-IND. While determining suspicious transactions, the company shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

Here, "Suspicious transaction" as defined in the PML rules; means a transaction including an attempted transaction, whether or not made in cash, which to a person acting in good faith

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified Complexity; or
c. appears to have no economic rationale or bona fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Explanation - Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

I. The company has identified a list of indicative circumstances to identify whether a particular transaction is suspicious or not depending upon the background, details of the transactions and other facts and circumstances:

   a. Clients whose identity verification seems difficult or clients that appear not to cooperate;
   b. Clients based in high risk jurisdictions;
   c. Substantial increases in business without apparent cause;
   d. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
   e. Attempted transfer of investment proceeds to apparently unrelated third parties;
   f. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.
   g. Prospective clients or who do not carry on the transaction after being informed about the KYC requirements of in-person meeting, verification of original OVD or who provide minimal, false or inconsistent information.

h. Clients or subscribers who provide false identification documents or documents that appears to be forged or inaccurate.
i. Clients or subscribers who use complex legal structures to hide the identity of the actual beneficial owner.
j. Clients or subscribers whose details match those reported in local media or open sources for criminal offenses or terrorism.
k. Clients or subscribers who cannot satisfactorily explain the source of their funds, or whose transactions involve movement of funds that is inconsistent with their business.
l. Transactions that have no economic rationale, or whose frequency, amount, or stated reason does not make sense for the particular client.
m. Clients or subscribers who have been the subject of an inquiry by any law enforcement agency relating to criminal offenses.
n. Clients or subscribers who make inquiries or attempt to convince staff to avoid reporting any of the above red flags.

II. Any suspicious transaction shall be immediately notified to thePrincipal Officer. The notification shall be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. 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. In exceptional circumstances, consent may not be given to continue the transaction and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

III. The Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

IV. In cases where transactions are abandoned or aborted by clients on being asked to give some details or to provide documents; the company shall report all such attempted transactions in Suspicious transaction Reporting, even if not completed by clients, irrespective of the amount of the transaction.

V. The company shall ensure that clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards published by FATF on its website (wwww.fatf-gafi.org)and which have been categorized as 'CSC' by regulators, are subject to appropriate counter measures. These measures shall include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

VI. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as d-mat account, security account maintained by the company. Record of all transactions where any forgery of a valuable security has taken place.

11.RECORD MANAGEMENT

Information to be maintained

The company is required to maintain and preserve the following information in respect of transactions referred to in PML Rules:

a. the nature of the transactions.
b. the amount of the transaction and the currency in which it is denominated;
c. the date on which the transaction was conducted; and
d. the parties to the transaction.

11.1. Record Keeping

a. The company shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

b. The company shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

c. It should be noted that in case of any suspected laundered money or terrorist property, the abovementioned records may be needed by, the competent investigating authorities to trace through the audit trail for reconstructing a financial profile of the suspect client. To enable this reconstruction, the company shall retain the following information of their clients in order to maintain a satisfactory audit trail:

   i. the beneficial owner of the client;
   ii. for selected transactions:
      a. the origin of the funds
      b. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
      c. the identity of the person undertaking the transaction;
      d. the destination of the funds;
      e. the form of instruction and authority.

d. The company shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, it shall retain certain records, e.g. client identification, and business correspondence, for periods which may exceed those required under the relevant Acts, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

e. The company shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under PML Rules as mentioned below:

   i. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non- monetary account such as demat account, security account maintained by the company.

11.2. Retention of Records

a. The company shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in PML Rules shall be maintained and preserved for a period of five years from the date of transactions between the client and company.

b. The company shall formulate and implement the CIP containing the requirements as laid down in the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as transaction files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and the company has ended

c. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

d. The company shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under PML Rules, for a period of five years from the date of the transaction between the client and the company.

12. PROCEDURE FOR FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES

The company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, company do not carry on any transactions with the individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

13. PROCEDURE FOR IMPLEMENTATION OF SECTION 12A OF THE WEAPONS OF MASS DESTRUCTION AND THEIR DELIVERY SYSTEMS (PROHIBITION OF UNLAWFUL ACTIVITIES) ACT, 2005:

1. The Ministry of Finance, Government of India, has issued an order dated September 01, 2023, detailing the procedure for implementing Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act). This order, accessible via the provided link DoR_Section_12A_WMD.pdf., must be strictly followed.

   As per Section 12A of the WMD Act, the Central Government is authorized to:

   a. Freeze, seize, or attach funds, financial assets, or economic resources owned, controlled, or derived from prohibited activities related to weapons of mass destruction.

   b. Prohibit the provision of funds, financial assets, or economic resources or related services for the benefit of individuals or entities involved in prohibited activities under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

2. The Company is obligated to adhere to the procedure outlined in the government order.

3. Key Responsibilities of the Company:

   a. Maintain the list of individuals/entities (“Designated List”) and update it, without delay.

   b. Verify if the particulars of the entities/individual, party to the financial transactions, match the particulars of the Designated List and in case of match, the Company shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to Central Nodal Officer (“CNO”), without delay. The details of CNO are as under:

      The Director
      FIU-INDIA
      Tel.No .: 011-23314458, 011-23314459 (Fax)
      Email: dir@fiuindia.gov.in

   c. Run a check, on the given parameters, at the time of establishing a relation with a client and on a periodic basis to verify whether individuals and entities in the Designated List are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, insurance policies etc. In case, the clients’ particulars match with the particulars of Designated List, the Company shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books to the CNO, without delay.

   d. The Company to send a copy of the communication, mentioned in paragraphs 3(b) and 3(c) above, without delay, to the Nodal Officer of SEBI. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the Nodal Officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, “G” Block, Bandra Kurla Complex, Bandra (E), Mumbai 400051;

   e. Prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, in case there are reasons to believe beyond doubt that funds or assets held by a client would fall under the purview of Section 12A (2)(a) or Section 12A(2)(b) of the WMD Act;

   f. File a Suspicious Transaction Report (STR) with the FIU-IND , covered under paragraphs 3(b) and (c) above, carried through or attempted through.

   g. Upon the receipt of the information above, the CNO would cause a verification to be conducted by the appropriate authorities to ensure that the individuals/entities identified are the ones in the Designated List and the funds, financial assets or economic resources or related services, reported are in respect of the designated individuals/entities. In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under section 12A would be issued by the CNO and be conveyed to the concerned reporting entity so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/entities.

h. The Company shall also comply with provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

14.List of Designated Individuals/ Entities

a. The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. The Company shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

b. All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by Regulators from time to time shall be taken note of for compliance.

c. An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at https://press.un.org/en/content/press-release

d. The details of the lists are as under:

i. 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://www.un.org/securitycouncil/sanctions/1267/press-releases.

ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases .

The company shall ensure that transactions are not carried on with anyone whose name appears in said list.

e. The company shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried by individuals/entities covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

f. Full details of transaction bearing resemblance with any of the individuals/entities in the list shall be intimated to the Central designated Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

g. The company shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the transaction is conducted and to SEBI and FIU-IND. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

<u>Jurisdictions that do not or insufficiently apply the FATF Recommendations</u>

a. The company shall put in place additional / increased monitoring of clients / transactions emanating from jurisdictions with strategic deficiencies in their regimes to counter money laundering, terrorist financing and proliferation of financing risks as per public statements released by FATF Secretariat & circulated by Regulators from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations.

b. The company shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the regulated entities are not precluded while entering / having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

15.Reporting to Financial Intelligence Unit-India

a. In terms of the PML Rules, the company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND). While reporting cash and suspicious transactions, the company shall adhere to the following:

i. The Cash Transaction Report (CTR) (Wherever applicable) for each month shall be submitted to FIU-IND by the 15th of the succeeding month.

ii. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. Principal Officer shall on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director in respect of transactions referred to in the PML Rules. 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.

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

iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.

vi. No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported.

“Non-profit organization” means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

vii. The company, including its Directors, officers, and all employees, shall ensure that the maintenance of records and the furnishing of information to the Director remain confidential.

viii. This confidentiality requirement does not prohibit the sharing of information required under the “policies by groups” of the PML Rules. Specifically, any analysis of transactions and activities that appear unusual can be shared, provided such analysis has been conducted.

b. The company shall not put any restrictions on transacting with the client where an STR has been made. The company and its directors, officers and employees (permanent and temporary) are prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

c. The company shall, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified PMLA Act, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime;

Wherein "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

Confidentiality requirement does not inhibit information sharing among entities in the group.

16.PERSONNEL HIRING / RECRUITMENT AND TRAINING / INVESTOR EDUCATION

16.1. Personnel Hiring / Recruitment:

The company shall have adequate screening procedures in place to ensure high standards when hiring & recruitment of relevant personnel. The Company shall identify the key positions within organization structures having regard to the risk of MF/TF and the size of business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

16.2. Training:

The company shall have an ongoing training programme so that the members of the staff are adequately trained in AML and CFT procedures.Training requirements shall have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients as 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.

16.3. Investor Education:

Implementation of AML/CFT measures requires the Company to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This 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 registered intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. The Company shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

17.INTERNAL CONTROL/AUDIT:

The Company shall get its procedures and processes to monitor ML activity; periodically audited to verify compliance with the extant policies, procedures and controls relating to the prevention of ML and TF.

The company shall place suggestions / comments/ notes of auditor with regards to robustness of the internal policies and processes along with steps taken to strengthen the policy and implementation aspects before the Audit Committee / Board of company.

Policy Approval & Review:

The policy shall be approved by the board of the company and shall be periodically reviewed and updated as per requirement and on the basis of amendments in relevant Rules, Regulations, Byelaws and Circulars as issued by regulatory authorities. Further, policy shall be reviewed at least once in a year by the Board of company.

This Policy last reviewed & approved on January 21, 2026