Allvest Securities Private Limited

PREVENTION OF MONEY LAUNDERING POLICY

Document Revision and Version Control

Version no	Month	Prepared by	Reviewed by	Adopted in Board
Ver 1	Feb 2026	Kandarp Padh	Amit Bansal	23/02/2026

TABLE OF CONTENTS

INTRODUCTION/ BACKGROUND

Allvest Securities Private Limited (hereinafter referred to as "ASPL" or "Company") is incorporated under the Companies Act, 2013, with Corporate Identification Number (CIN) U66120MH2025PTC440678. ASPL is registered as Stock Broker with SEBI having Registration number INZ000330839 and is registered as Trading Cum Self Clearing Member with National Stock Exchange of India Ltd and NSE Clearing Ltd. (Member Code: 90469), as a Trading Member with BSE Ltd. (Member Code:6973), as a Trading Cum Self Clearing Member with Multi Commodity Exchange of India Limited (Member Code :57650) and ASPL is also registered with SEBI as a Depository Participant having Registration No.: IN-DP-837-2026 and with NSDL having DP ID: IN304949.

SCOPE

This Anti-Money Laundering (AML) Policy (the "Policy") has been established by ASPL in compliance with the Prevention of Money Laundering Act, 2002 (PMLA). The Policy also considers the provisions of the PMLA Act, as well as relevant rules set forth by regulatory bodies such as SEBI and the Financial Intelligence Unit (FIU). This Policy has been prepared in consideration to the Prevention of Money Laundering Act, 2002 followed by SEBI Master Circular No. SEBI/HO/ MIRSD/ MIR SD SE CF ATF/ P/ CIR/ 2024/78 dated June 06, 2024, respectively.

OBJECTIVE

This Policy is established by ASPL, in compliance with the Prevention of Money Laundering Act, 2002 (PMLA), and in alignment with global measures to combat money laundering (ML), terrorism financing (TF), and other serious crimes. This Policy ensures that ASPL follows effective procedures to prevent, detect, and report activities related to money laundering and terrorism financing, fulfilling its obligations as per statutory and regulatory requirements.

ASPL has put in place this Policy to ensure strict adherence to AML and CFT guidelines, protect the integrity of the financial system, and comply with the regulatory framework governing money laundering and terrorism financing activities. This includes adherence to all applicable provisions of the PMLA, as well as SEBI, FIU, and other regulatory bodies.

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 securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line

with these measures and mandates that all intermediaries ensure the fulfilment of the aforementioned obligations.

"**Group**" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of rule 2 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 as amended from time to time. Groups shall implement group-wide policies for the purpose of discharging obligations under chapter 4 of PMLA."

ASPL, as part of its PMLA compliance, has a structured group-wide AML/CFT framework to ensure robust money laundering (ML) and terrorist financing (TF) risk management across all its branches and majority-owned subsidiaries.

Key Measures:

- Information Sharing: Policies for seamless exchange of data related to Customer Due Diligence (CDD) and ML/TF risk management.
- Group-Level Oversight: Compliance, audit, and AML functions at the group level shall have access to customer, account, and transaction details when required for AML/CFT purposes. This includes monitoring and analyzing unusual transactions.
- Confidentiality & Security: Strong safeguards to maintain the confidentiality of exchanged information and prevent tipping-off.

ASPL ensures strict adherence to SEBI's PMLA guidelines for effective risk management within its financial group.

To be in compliance with these obligations, the senior management of ASPL is fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Accordingly, ASPL shall:

i. issue a statement of policies and procedures and implement, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;

ii. ensure that the content of these Directives are understood by all staff members;

iii. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;

iv. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;

v. undertake client due diligence ("CDD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

vi. have in system a place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and

vii. develop staff members' awareness & vigilance to guard against ML & TF

Policies and procedures to combat ML shall cover:

i. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handles account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;

ii. Client acceptance policy and client due diligence measures, including requirements for proper identification;

iii. Maintenance of records;

iv. Compliance with relevant statutory and regulatory requirements;

v. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and

vi. 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

vii. 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.

WRITTEN ANTI-MONEY LAUNDERING PROCEDURES

ASPL, shall adopt and implement written procedures to effectively fulfill its obligations under the Prevention of Money Laundering Act (PMLA). These procedures are designed to ensure the detection and prevention of money laundering (ML) and terrorist financing (TF) risks and shall be reviewed and updated regularly.

The procedures shall focus on the following key areas, related to the Client Due Diligence (CDD) process:

i. policy for acceptance of clients;

ii. procedures for identifying the clients; and

iii. Risk Management;

iv. transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

CLIENT DUE DILIGENCE (CDD) PROCEDURES

Client Due Diligence (CDD) refers to the process of conducting necessary checks on a client to ensure they are not involved in money laundering or terrorist financing activities. These checks are carried out using reliable and independent sources of information, and the procedures aim to identify the true beneficial owners of the client and/or account holder.

ASPL's CDD measures are designed to manage and mitigate the risks of ML and TF, considering the nature of the client, the risk profile, and the size of the business relationship, approved by the senior management. These measures include the following components:

1. **Obtaining Sufficient Information**

   - ASPL shall obtain sufficient and reliable information to identify all parties involved in the ownership or control of a securities account.

   - If the securities are beneficially owned by a party other than the client, that party shall be identified and verified using reliable sources, it also incorporates those person who exercise ultimate effective control over a legal person or arrangement.

2. **Verification of Client Identity**

   - ASPL will verify the identity of the client using reliable and independent sources, including official documents and data.

   - In cases where the client is acting on behalf of a juridical person (such as a company, or partnership), ASPL will verify the identity of the authorized person and their authority to act on behalf of the client. Provided that in case of trust, the reporting entity shall ensure that trustee disclose their status at the time of commencement of an account-based relationship.

3. **Identifying Beneficial Ownership**

   - The beneficial owner is the individual(s) who ultimately owns or controls a client and/or is on whose behalf a transaction is conducted. The beneficial ownership shall be determined in accordance with the following categories:

a) Company: If 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 person(s), has a controlling ownership interest or exercises control through other means.

Explanation:

- *Controlling Ownership Interest*: This refers to ownership of or entitlement to more than ten percent (10%) of the shares, capital, or profits of the company.
- *Control*: This includes the right to appoint a majority of directors, or to control the management or policy decisions of the company. This can occur through shareholding, management rights, shareholder agreements, or voting agreements.

b) Partnership Firm: If the client is a partnership firm, the beneficial owner is the natural person(s) who has ownership of or entitlement to more than ten percent (10%) of the capital or profits of the partnership, or who exercises control through other means.

Explanation:

- *Control*: This refers to the right to control the management or policy decisions of the partnership.

c) Unincorporated Association or Body of Individuals: If the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s) who has ownership of or entitlement to more than fifteen percent (15%) of the property, capital, or profits of such association or body of individuals.

d) Senior Managing Official: If no natural person is identified as the beneficial owner under the categories (a), (b), or (c), the beneficial owner shall be the relevant natural person who holds the position of senior managing official within the entity.

e) Trust: In the case of a trust, identification of the beneficial owner(s) shall include the identification of the following individuals:

- The author (settlor) of the trust.
- The trustee(s).
- Beneficiaries with ten percent (10%) or more interest in the trust.
- Any natural person exercising ultimate effective control over the trust through a chain of control or ownership, including the protector.

f) Listed Entities: If the client or the entity with the controlling interest is listed on a stock exchange in India or is a subsidiary of such a listed entity, or if it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

g) Applicability for Foreign Investors: Registered intermediaries dealing with foreign investors are required to adhere to the guidelines provided in the SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022, and any amendments thereto, for the identification of beneficial ownership of the client.

4. **Verification of Beneficial Ownership**

   - The beneficial owner shall be verified through corroborated sources, and ongoing due diligence will be performed to ensure that the transactions align with the client's knowledge, business, and risk profile.

5. **Understanding Client's Business and Ownership Structure**

   - ASPL will ensure that it fully understands the nature of the client's business, ownership structure, control structure and any relevant relationships to prevent potential risks associated with ML/TF.

6. **Ongoing Due Diligence and Scrutiny**

   - Continuous monitoring of client transactions and accounts will be conducted to ensure that they are consistent with the client's risk profile and business activities.

   - Suspicious transactions or activities will be flagged, and the CDD process will be reviewed if there are concerns regarding potential money laundering or terrorist financing.

7. **Periodic Updating of Client Information**

   - ASPL will periodically review and update the information and documentation collected during the CDD process to ensure that it remains accurate and relevant, especially for high-risk clients.

   - Updates will also be made in situations where doubts arise about the adequacy or authenticity of previous client information.

8. **Action on Suspicious Transactions**

   - If ASPL suspects that a transaction is related to money laundering or terrorist financing, and performing further CDD may tip off the client, it will refrain from pursuing additional CDD and instead file a **Suspicious Transaction Report (STR)** with the Financial Intelligence Unit (FIU-IND).

9. **Special Measures for Non-Profit Organizations (NPOs)**

- For clients that are non-profit organizations, ASPL will ensure that they are registered on the DARPAN Portal of NITI Aayog (if not already registered) and will retain such records for a period of five years after the business relationship between a client and ASPL has ended or the account has been closed, whichever is later.

10. **Suspicion of Money Laundering or Terrorist Financing**:

- In situations where ASPL, has reasonable suspicion that a transaction is linked to money laundering or terrorist financing, the Suspicious Transaction Report (STR) will be filed with Financial Intelligence Unit of India (FIU-IND) as per regulatory requirements within 7 days from the suspicion is established.

- Further, ASPL will tip-off the client and maintain confidentiality about filing of the STR.

11. **Obligation to Follow CDD Procedure**:

- ASPL will ensure that no transaction or account-based relationship is undertaken without first completing the required Customer Due Diligence (CDD) procedure, in line with regulatory compliance.

POLICY FOR ACCEPTANCE OF CLIENTS

ASPL shall establish and implement comprehensive client acceptance policies and procedures to identify clients who may pose a higher than average risk of money laundering (ML) or terrorist financing (TF). These policies ensure that ASPL apply client due diligence (CDD) on a risk-sensitive basis, depending on the type of client, business relationship, or transaction. The following safeguards shall be followed while accepting clients:

i. **No Anonymous Accounts:** ASPL will not permit the opening or maintenance of any anonymous accounts, fictitious accounts, or accounts opened on behalf of other persons whose identity has not been disclosed or cannot be verified.

ii. **Risk Perception Factors:** ASPL shall clearly define factors to assess the risk perception of clients, considering their location (e.g., registered office, correspondence addresses), nature of business activity, trading turnover, and the manner of payment for transactions. Clients will be classified into low, medium, and high-risk categories based on these parameters. In order to achieve this objective, all clients should be classified in the following category:

- Category A – High risk
- Category B – Medium Risk
- Category C – Low risk

iii. **Enhanced Due Diligence for Clients of Special Category (CSC):** Clients of Special Category (CSC) will undergo enhanced due diligence measures. Clients from special categories (listed below) may be classified as High Risk and will require enhanced due diligence and regular updates to their Know Your Customer (KYC) profiles. CSC includes the following categories:

- Non-resident clients
- High net-worth clients
- Trusts, Charities, Non-Governmental Organizations (NGOs), and organizations receiving donations
- Companies with close family shareholding or beneficial ownership
- Politically Exposed Persons (PEPs), as defined in the PML Rules, including family members and close associates of PEPs
- Clients in high-risk countries (as identified by the Financial Action Task Force (FATF) and publicly available information)
- Non-face-to-face clients (clients who do not meet intermediaries in person, including those utilizing video-based customer identification processes)
- Clients with dubious reputations, as indicated by public information

ASPL shall independently assess clients who fall outside of these categories and apply appropriate due diligence.

iv. **Documentation Requirements:** The necessary documentation and information will be collected depending on the perceived risk of the client, in line with Rule 9 of the PML Rules and the directives issued by SEBI.

v. **Accounts Where CDD Cannot Be Applied:** ASPL shall not open an account if it is not possible to apply appropriate CDD measures. This includes situations where the identity of the client cannot be ascertained, or the provided information is suspected to be false, or if the client is uncooperative. If these issues arise, the ASPL shall not continue the business relationship and will file a Suspicious Activity Report (SAR). ASPL shall also evaluate any suspicious trading and consider whether to freeze or close the account in such circumstances.

vi. **Client Acting on Behalf of Another Entity:** If a client is acting on behalf of another person or entity, the circumstances will be clearly outlined. The account's operation, transaction limits, and additional authority requirements for transactions above specified thresholds will be defined. The rights and responsibilities of both the persons, i.e., the agent-client registered with ASPL, as well as the person on whose

behalf the agent is acting, shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

vii. **Client Background Checks:** ASPL will conduct necessary checks to ensure that the client's identity does not match any individual with a known criminal background or who is banned from conducting business due to criminal or civil proceedings by enforcement agencies worldwide.

viii. **Revisiting CDD Process:** The CDD process will be revisited when there are suspicions of money laundering or terrorist financing, ensuring continuous compliance and risk management.

CLIENT IDENTIFICATION PROCEDURE (CIP)

1. **Client Identification Procedure (CIP) Framework**: ASPL shall have a clear and comprehensive Client Identification Procedure (CIP) in place, which shall be followed at different stages:
    - At the time of establishing the intermediary-client relationship,
    - While carrying out transactions for the client,
    - When ASPL has doubts regarding the veracity or adequacy of previously obtained client identification data.
2. **Compliance Requirements for CIP**: ASPL, shall ensure compliance with the following requirements while implementing the CIP:
    i. **Politically Exposed Persons (PEP) Identification**: ASPL shall proactively establish appropriate risk management systems to determine if the client, potential client, or beneficial owner is a Politically Exposed Person (PEP). The procedures will include:
        - Seeking relevant information from the client,
        - Referring to publicly available information,
        - Accessing commercial electronic databases of PEPs.

    ii. **Senior Management Approval for PEPs**
        - ASPL shall obtain senior management approval to establish business relationships with PEPs.
        - If a client or beneficial owner is found to be, or becomes, a PEP after the relationship is established, senior management approval shall be obtained to continue the business relationship.

iii. **Verification of Sources of Funds and Wealth for PEPs**: ASPL shall take reasonable measures to verify the sources of funds and wealth of clients and beneficial owners identified as PEPs.

iv. **Client Identification and Information Collection**: ASPL shall identify each client using reliable sources of information and documents. Adequate information will be obtained to clearly establish the identity of each new client and the purpose of the intended business relationship.

v. **Adequacy of Information for Regulatory Scrutiny**: The information obtained must be sufficient to satisfy regulatory and enforcement authorities that due diligence was observed. Original documents must be examined before accepting a copy.

vi. **Non-compliance by Prospective Clients**: In the event that a prospective client fails to provide satisfactory evidence of identity, this shall be noted and reported to the higher authorities within ASPL for further action.

3. **KYC Compliance**: ASPL shall adhere to the minimum KYC requirements specified by SEBI and any subsequent amendments. Based on these requirements, ASPL shall develop and implement its own internal directives in line with its experience in dealing with clients and legal obligations.

4. **Ongoing Due Diligence**: ASPL will conduct ongoing due diligence, especially when inconsistencies are noticed in the information provided by the client. The objective is to comply with the requirements of the Prevention of Money Laundering Act (PMLA), the SEBI Act, and any other applicable regulations and directives to ensure that ASPL is aware of the clients it is dealing with.

5. **CIP and PML Rules Compliance**: ASPL shall formulate and implement a Client Identification Procedure (CIP) that complies with the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005, as amended. This includes:

    - Maintenance of records regarding the nature and value of transactions,
    - Procedures for maintaining and furnishing information and verifying the records of client identity,
    - Ensuring full compliance with SEBI and PMLA regulations, regardless of the investment amount made by clients.

ASPL shall not have any minimum threshold or exemptions available for obtaining the necessary information/documents from clients as prescribed by the PML Rules or SEBI Circulars. No category of clients will be exempt from undergoing the full Customer Due Diligence (CDD) process and this shall be strictly implemented by ASPL.

6. **Non-compliance Consequences**: Any non-compliance with the above CIP policy shall result in appropriate sanctions, in accordance with the regulatory framework and applicable guidelines.

RELIANCE ON THIRD PARTY FOR CARRYING OUT CLIENT DUE DILIGENCE (CDD)

Third-Party Reliance for Client Due Diligence (CDD): ASPL may, under specific circumstances, rely on a third party for the following aspects of the Client Due Diligence (CDD) process:

- **Identification and verification** of the client's identity.
- **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 PML Act

Conditions for Reliance on Third Party (as per Rule 9(2) of PML Rules): Any reliance on a third party for CDD shall be subject to the conditions outlined in Rule 9(2) of the PML Rules and the relevant regulations, circulars, and guidelines issued by SEBI. In terms of Rule9(2) of PML Rules:

i. **Obtaining Information on CDD from Third Party**

- ASPL shall immediately obtain necessary information regarding the client due diligence carried out by the third party.

ii. **Availability of Documentation upon Request**

- ASPL shall take adequate steps to ensure that the third party will provide copies of identification data and other relevant documentation related to client due diligence upon request, without delay.

iii. **Third Party's Compliance Measures**

- ASPL shall confirm that the third party is regulated, supervised, or monitored, and has the necessary measures in place to comply with client due diligence and record-keeping requirements in accordance with the PML Act.

iv. **Jurisdictional Risk Assessment**

- The third party must not be based in a country or jurisdiction that is assessed as high risk.

v. **Ultimate Responsibility for CDD**

- ASPL shall remain ultimately responsible for performing CDD and ensuring that enhanced due diligence measures are applied as needed.

RISK MANAGEMENT

1. RISK-BASED APPROACH (RBA)

ASPL shall adopt a Risk-Based Approach (RBA) to manage and mitigate identified risks, ensuring policies, controls, and procedures are approved by senior management. The key components of this approach include:

- ASPL will have documented policies and controls in place, which will be regularly reviewed and updated as necessary to manage the risk effectively.
- Continuous monitoring of the implementation of these controls will be conducted to ensure they are functioning effectively.

Client Due Diligence Based on Risk Sensitivity: Recognizing that clients pose varying levels of risk, ASPL will apply client due diligence measures on a risk-sensitive basis. The principles of this approach include:

- **Enhanced Due Diligence (EDD)** will be applied to higher-risk clients, which may include clients with complex structures or from high-risk regions.
- **Simplified Due Diligence (SDD)** may be applied to lower-risk clients, where the risk of money laundering or terrorist financing is minimal.
- **Tailored Information:** The type and volume of information required for identification and verification will be proportional to the risk category of the client.

Low-Risk Provisions and Suspicion of ML/TF: ASPL will ensure that low-risk provisions do not apply when there are suspicions of money laundering (ML) or terrorist financing (TF). If any factors suggest that a customer does not truly pose a low risk, ASPL will increase the due diligence accordingly.

2. RISK ASSESSMENT

ASPL will carry out a comprehensive risk assessment to identify, assess, and mitigate the risks related to money laundering and terrorist financing (ML/TF), including:

- **Client Risk Factors:** Assessing risks related to clients based on their business nature, geographical location, transaction volume, and payment methods.
- **Country/Geographical Risks:** Identifying risks associated with clients in high-risk countries or regions.

- **Transaction Methods:** Assessing the methods clients use to conduct transactions, especially if they involve unusual or complex financial structures.

Risk Assessment Process: ASPL 's risk assessment will be carried out with the following key steps:

- **Identification of Risks:** All relevant risk factors will be considered when determining the overall risk level and the type of mitigation measures to be applied.
- **Documentation:** The assessment will be well-documented, regularly updated, and available for review by competent authorities or self-regulatory bodies when required.
- **Ongoing Updates:** Regular updates will be conducted to ensure that new risk factors or changes in business or regulatory environments are addressed.

Risk Assessment for New Products and Practices: ASPL will carry out risk assessments before the launch or adoption of new products, services, or technologies, and in relation to new business practices or delivery mechanisms. This will include:

- **Risk Assessment Prior to Launch:** A thorough assessment of ML/TF risks associated with new offerings will be conducted before they are launched.
- **Ongoing Risk Management:** A risk-based approach will be used to manage and mitigate any risks that arise in relation to new technologies or business practices.

Country-Specific and Sanction Lists: The risk assessment will include consideration of:

- **Country-Specific Information:** Any country-specific risks as circulated by the Government of India, SEBI, or other relevant authorities.
- **Sanction Lists:** The updated list of individuals and entities subject to sanctions under United Nations Security Council Resolutions and relevant laws will be regularly reviewed and incorporated into the risk assessment.

MONITORING OF TRANSACTIONS

ASPL commits to the regular monitoring of client transactions as an essential part of ensuring the effectiveness of Anti-Money Laundering (AML) procedures, by having a clear understanding of the typical activity patterns of each client. By doing so, ASPL is able to identify deviations from normal activity, which may indicate suspicious transactions.

ASPL shall pay special attention to complex or unusually large transactions, or transaction patterns that appear to lack an apparent economic purpose. In addition,

ASPL may also establish internal threshold limits for various categories of client accounts. Transactions that exceed these limits will be scrutinized more closely.

Supporting documentation, including office records, memorandums, and clarifications regarding these transactions, will be reviewed thoroughly. All findings will be documented in writing. These findings, along with supporting records and relevant documents, will be made available to auditors and regulatory authorities such as SEBI, stock exchanges, FIU-IND, or other relevant bodies during audits, inspections, or as required.

ASPL shall apply client due diligence (CDD) measures to both new and existing clients. For existing client relationships, CDD will be carried out based on materiality and risk assessment. The extent of transaction monitoring will be tailored to the specific risk category of each client.

ASPL will ensure that transaction records are maintained in compliance with Section 12 of the Prevention of Money Laundering Act (PMLA). Any transactions deemed suspicious, or any other transactions identified for reporting under Section 12, will be promptly reported to the Director of the Financial Intelligence Unit – India (FIU-IND).

Additionally, all suspicious transactions will be escalated and reported to senior management within ASPL for further review and appropriate action.

Further, the compliance cell of ASPL 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.

Suspicious Transaction Monitoring and Reporting

Recognition of Suspicious Transactions: ASPL shall take appropriate steps to ensure that suspicious transactions are recognized and reported in a timely manner. In determining whether a transaction is suspicious, ASPL will be guided by the definition of a suspicious transaction as set forth in the PML Rules, as amended from time to time.

Illustrative Circumstances of Suspicious Transactions: The following list includes circumstances that may indicate suspicious transactions. This list is non-exhaustive, and whether a particular transaction is suspicious will depend on the background, details of the transactions, and other facts and circumstances:

i. Clients whose identity verification is difficult or who appear to be uncooperative.
ii. Asset management services for clients where the source of funds is unclear or inconsistent with the client's apparent standing or business activity.
iii. Clients based in high-risk jurisdictions.
iv. Substantial increases in business volume without an apparent cause.
v. Clients transferring large sums of money to or from overseas locations, with instructions for payment in cash.

vi. Attempted transfers of investment proceeds to apparently unrelated third parties.
vii. Unusual transactions by Corporate Service Providers (CSCs) and businesses conducted by offshore banks/financial services.

Reporting of Suspicious Transactions: Any suspicious transaction identified shall be immediately reported to the Designated/Principal Officer within ASPL. The report should include specific details regarding the client, the transaction, and the nature/reason for suspicion.

While awaiting further investigation, normal business relationships with the client will continue unless otherwise instructed. Clients will not be informed of any suspicions or reports being made.

In exceptional circumstances, consent may be withheld, and transactions may be suspended in one or more jurisdictions, or other actions may be taken. The Designated/Principal Officer, along with compliance, risk management, and other relevant staff, shall have timely access to all necessary client identification data, client due diligence (CDD) information, transaction records, and other pertinent documents.

Reporting of Abandoned or Aborted Transactions: In cases where a transaction is abandoned or aborted by a client on being asked to give some details or to provide any additional documents, ASPL will still report these attempted transactions as Suspicious Transaction Reports (STRs), even if the transaction was not completed, irrespective of the amount of the transaction.

Enhanced Measures for High-Risk Countries: ASPL recognizes that clients from high-risk countries (those where the effectiveness of money laundering controls is questionable or where FATF standards are not fully applied) are subject to heightened scrutiny. In line with paragraph 18(iii)(f) of the relevant regulatory circular, such clients (referred to as 'CSC' clients) will be subject to appropriate countermeasures, which may include:

- Enhanced scrutiny of transactions involving these clients.
- Enhanced reporting mechanisms or systematic reporting of financial transactions.
- Application of enhanced due diligence when expanding business relationships with persons or entities from these countries.

RECORD MANAGEMENT

Information to be Maintained

ASPL shall maintain and preserve the following information in respect of transactions as required under Rule 3 of the PML Rules:

i. The nature of the transaction.
ii. The amount of the transaction and the currency in which it is denominated.
iii. The date on which the transaction was conducted.
iv. The parties involved in the transaction.

Record Keeping Requirements

ASPL shall comply with the record-keeping requirements under the SEBI Act, 1992, the PMLA, and other relevant legislation, rules, regulations, exchange bye-laws, and circulars.

ASPL shall ensure that records are maintained in a manner sufficient to reconstruct individual transactions. This includes retaining records of the amounts and types of currencies involved, as well as providing the necessary evidence for the prosecution of any criminal activity related to money laundering or terrorism financing.

In case of any suspected laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable authorities to reconstruct a financial profile of a suspect account, ASPL shall retain the following details for each client account in order to maintain the satisfactory audit trail:

i. The beneficial owner of the account.
ii. The volume of funds flowing through the account.
iii. 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).
   c. The identity of the person conducting the transaction.
   d. The destination of the funds.
   e. The form of instruction and authority.

Availability of Records to Authorities: ASPL shall ensure that all client and transaction records are available on a timely basis to competent investigating authorities. If required, the company shall retain certain records, such as client identification, account files, and business correspondence, for periods exceeding those stipulated by the SEBI Act, PMLA, or other applicable regulations.

ASPL shall maintain a system for recording and preserving the following types of transactions:

i. All cash transactions exceeding ten lakh rupees or its equivalent in foreign currency.

ii. Any series of cash transactions that are integrally connected and have a monthly aggregate exceeding ten lakh rupees, even if individual transactions are below this threshold.

iii. All cash transactions involving forged or counterfeit currency notes, bank notes, or valuable securities or documents facilitating the transaction.

iv. All suspicious transactions, regardless of whether they are made in cash. This includes credits or debits into or from non-monetary accounts such as demat or security accounts maintained by ASPL.

It is clarified that, for the purpose of suspicious transaction reporting, not only "integrally connected" transactions but also "remotely connected or related" transactions will be considered.

In cases where ASPL does not possess records of the identity of its existing clients, the company shall obtain these records immediately. If such records cannot be obtained, ASPL will close the client's account after providing due notice to the client.

Explanation: "Records of the identity of clients" shall include updated identification details, account files, business correspondence, and any analysis conducted under Rules 3 and 9 of the PML Rules.

Retention and Preservation of Records

ASPL shall develop and implement an internal mechanism for the proper maintenance and preservation of client and transaction records. This mechanism will ensure that records are stored in a manner that facilitates easy and quick retrieval upon request by competent authorities.

In accordance with Rule 3 of the PML Rules, ASPL shall maintain and preserve transaction-related records for a period of five years after the business relationship between a client and ASPL has ended or the account has been closed, whichever is later. This includes records related to the nature, amount, currency, date, and parties involved in each transaction.

In cases where records pertain to ongoing investigations or transactions that are the subject of suspicious transaction reports (STRs), these records shall be retained until the investigating authorities confirm that the case has been closed.

ASPL will retain records related to transactions that have been reported to the Director, FIU-IND, as required under Rules 7 and 8 of the PML Rules. These records will be preserved for a period of five years from the date of the transaction between the client and ASPL.

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

ASPL shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have any accounts in the name of 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).

In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, the Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1)for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2). Corrigenda dated March 15, 2023, and April 22, 2024, have also been issued in this regard (Annexure 3) and (Annexure 4). The list of Nodal Officers for UAPA is available on the website of MHA.

PROCEDURE FOR IMPLEMENTATION OF SECTION 12A OF THE WEAPONS OF MASS DESTRUCTION AND THEIR DELIVERY SYSTEMS (PROHIBITION OF UNLAWFUL ACTIVITIES) ACT, 2005 – DIRECTIONS TO STOCK EXCHANGES AND REGISTERED INTERMEDIARIES

The Government of India, Ministry of Finance has issued an order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") detailing the procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"). The Order may be accessed by clicking on DoR_Section_12A_WMD.pdf.

In terms of Section 12A of the WMD Act, the Central Government is empowered as under: "(2) For prevention of financing by any person of any activity which is prohibited 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, the Central Government shall have power to—

(a) Freeze, seize or attach funds or other financial assets or economic resources—

i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or
ii. held by or on behalf of, or at the direction of, such person; or
iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

(b) Prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited 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.

The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

ASPL is directed to comply with the procedure laid down in the said Order.

ASPL shall:

i. Maintain the list of individuals/entities ("Designated List") and update it, without delay, in terms of paragraph 2.1 of the Order.
ii. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, ASPL 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 the Central Nodal Officer ("CNO"), without delay. The details of the CNO are as under:

    The Director FIU-INDIA
    Tel.No.: 011-23314458, 011-23314459 (FAX)
    Email: dir@fiuindia.gov.in
iii. ASPL shall 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 the Designated List, ASPL 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.

iv. ASPL will send a copy of the communication mentioned in paragraphs 59(ii) and 59(iii) 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 400 051.

v. ASPL will 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.

vi. ASPL will file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered under paragraphs 59(ii) and (iii) above, carried through or attempted through.

ASPL shall comply with the provisions regarding exemptions from the orders of the CNO and inadvertent freezing of accounts, as may be applicable.

List of Designated Individuals/ Entities

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'. ASPL shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

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

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. The details of the lists are as under:

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

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

The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea is available at:

www.un.org/securitycouncil/sanctions/1718/press-releases.

ASPL is directed to ensure that accounts are not opened in the name of anyone whose name appears on said list. ASPL shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

ASPL shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets, or economic resources or related services held in the form of securities with them.

ASPL shall leverage the latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

ASPL shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35(1) and 51A of UAPA.

Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately 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.

ASPL shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay. 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 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

JURISDICTIONS THAT DO NOT OR INSUFFICIENTLY APPLY THE FATF RECOMMENDATIONS

FATF Secretariat after conclusion of each of its plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by ASPL.

ASPL 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 ASPL is not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA

In terms of the PML Rules, ASPL is required to report information relating to cash and 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, INDIA
Telephone: 91-11-23314429, 23314459
91-11-23319793(Helpdesk) Email: helpdesk@fiuindia.gov.in

(For FINnet and general queries) ctrcell@fiuindia.gov.in

(For Reporting Entity / Principal Officer registration related queries) complaints@fiuindia.gov.in

Website: http://fiuindia.gov.in

ASPL shall carefully go through all the reporting requirements (https://www.sebi.gov.in/sebi_data/commondocs/jun2024/Brochures on FIU_p.pdf) and formats that are available on the website of FIU – IND under the Section Home - FINNET 2.0 – User Manuals and Guides - Reporting Format (https://www.sebi.gov.in/sebi_data/commondocs/jun2024/Reporting_Format_p.pdf). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND.

The related hardware and technical requirements for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, ASPL shall adhere to the following:

- The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- 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. The 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 clause (D) of sub-rule (1) of rule 3 of 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.
- The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- The Principal Officer will be responsible for timely submission of CTR, STR, and NTR to FIU-IND.
- ASPL shall maintain utmost confidentiality while filing CTR, STR, and NTR to FIU-IND.
- No NIL reporting needs to be made to FIU-IND in case there are no cash/suspicious/non-profit organization transactions to be reported.
- The NTR counts needs & even the NIL reporting needs to be made on ePASS portal of NSDL on or before 20th of the succeeding month.

- STR count & even the NIL reporting needs to be made on BEFS portal on or before 7th of the succeeding month.

- ASPL shall ensure that the fact of maintenance referred to in Rule 3 of PML Rules and furnishing of information to the Director is kept confidential. Provided that nothing in this rule shall inhibit sharing of information under Rule 3A of PML Rules of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

ASPL shall not put any restrictions on operations in the accounts where an STR has been made. ASPL and their directors, officers, and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that an 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.

It is clarified that ASPL, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of the Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

Confidentiality requirements do not inhibit information sharing among entities in the group.

Designation of officers for ensuring compliance with provisions of PMLA Appointment of a Principal Officer

To ensure that ASPL properly discharges its legal obligations to report suspicious transactions to the authorities, ASPL shall appoint a senior person at the management level as the Principal Officer who would 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. The Principal Officer 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 the 'Principal Officer', including any changes therein, shall also be intimated to the Office of the Director-FIU-IND.

Appointment of a Designated Director

In addition to the existing requirement of designation of a Principal Officer, ASPL shall also designate Managing Director or a Whole-Time Director or other appropriate senior person duly authorized by the Board of Directors of ASPL as the 'Designated Director'.

ASPL shall communicate the details of the Designated Director, such as name, designation, and address, to the Office of the Director, FIU – IND.

Hiring and Training of Employees and Investor Education

Hiring of Employees: ASPL shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

Training of Employees: ASPL shall have an ongoing employee training program 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. 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.

Investor Education: Implementation of AML/CFT measures requires ASPL 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 the source of funds/income tax returns/bank records etc. This can sometimes lead to raising questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need for ASPL to sensitize their clients about these requirements as the ones emanating from the AML and CFT framework. ASPL shall prepare specific literature/pamphlets etc. so as to educate the client on the objectives of the AML/CFT program.

Review of the policy and Update

The policy will be reviewed and updated as required to incorporate any changes introduced by regulatory authorities. Additionally, it will undergo periodic review at least once in a year to ensure its continued relevance, effectiveness, and alignment with current regulatory requirements and industry standards by the Board.

xxxxxxxxxxxxxxxxxxx