AAA INSTITUTIONAL SECURITIES PVT LTD

Space On B-16-A, Plot No-5, Community Centre, New Friends Colony, New Delhi - 110065 | Tel. No.: 011 - 49948719 | Mob. No. +91-96677 38861

Email: info@aaa-securities.com | Website: www.aaa-securities.com

CIN: U66120DL2026PTC464792

ANTI MONEY LAUNDERING POLICY (AML)

CIN: U66120DL2026PTC464792
Website: https://aaa-securities.com/
Registered Office: SPACEON B-16-A, PLOT N-5, COMM. CENTRE, SRINIWASPURI, SOUTH DELHI, DELHI, INDIA-110065
Contact: +91 9667738861
Email: compliance@aaa-securities.com

1. INTRODUCTION TO AML

The Directives as outlined below provide a general background and summary of the main provisions of the applicable anti-money laundering and anti-terrorist financing legislations in India. They also provide guidance on the practical implications of the Prevention of Money Laundering Act, 2002 (PMLA). The Directives also set out the steps that a registered intermediary or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities. These Directives are intended for use primarily by intermediaries registered under Section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act), Stock Exchanges, Depositories and other recognized entities under the SEBI Act and Regulations and rules there under. While it is recognized that a "one-size-fits-all" approach may not be appropriate for the securities industry in India, each registered intermediary shall consider the specific nature of its business, organizational structure, type of clients and transactions, etc. when implementing the suggested measures and procedures to ensure that they are effectively applied. The overriding principle is that they shall be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

2. BACKGROUND

This Policy has been framed by **AAA Institutional Securities Private Limited ("AAA")** in order to comply with the applicable Anti Money Laundering (AML) Standards/Combating the Financing of Terrorism (CFT)/Obligations of Securities Market Intermediaries under the Prevention of

Money Laundering Act, 2002 and pursuant to the recommendations made by the Financial Action Task Force on anti-money laundering standards.

SEBI had issued the Guidelines on Anti Money Laundering Standards vide their notification No. ISD/CIR/RR/AML/1/06 dated 18th January 2006, vide Circular No. ISD/CIR/RR/AML/2/06 dated 20th March 2006, vide letter No. ISD/AML/CIR-1/2008 dated December 19, 2008, vide Circular No. ISD/AML/CIR-1/2009 dated September 01, 2009, vide Circular No. ISD/AML/CIR-2/2009 dated October 23, 2009, vide Circular CIR/ISD/AML/3/2010 dated December 31, 2010, vide Circular No. ISD/AML/CIR-1/2010 dated February 2010, vide Circular number CIR/MIRSD/11/2014 dated March 12th, 2014, vide Circular SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated July 04th, 2018, vide Circular No. SEBI/HO/MIRSD/DOP/CIR/P2019/113 dated October 15, 2019, vide Circular No. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 and Circular No. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated June 16, 2023 and vide SEBI Circular No. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06, 2024 had issued the obligations of the intermediaries registered under Section 12 of SEBI Act, 1992.

AAA Institutional Securities Private Limited shall ensure that proper policy frameworks are put in place as per the Guidelines on Anti Money Laundering Standards notified by SEBI.

As per the provisions of PMLA and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (Maintenance of Records Rules), as amended from time to time and notified by the Government of India, every reporting entity (which includes intermediaries registered under section 12 of the SEBI Act, i.e. a stock-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the SEBI Act and stock exchanges), shall have to adhere to the client account opening procedures, maintenance records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

The Maintenance of Records Rules empowers SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and form in which it is to be

maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by the regulator for detecting the transactions specified in the Maintenance of Records Rules and for furnishing information thereof, in such form as may be directed by SEBI.

The PMLA inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as provided in Section 12A read with Section 24 of the SEBI Act will be treated as a scheduled offence under schedule B of the PMLA.

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

3.1 ESSENTIAL PRINCIPLES

These Directives have taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed Directives in Section II have outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. Each intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures in Section II and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.

In case there is a variance in Client Due Diligence (CDD)/Anti Money Laundering (AML) standards specified by SEBI and the regulators of the host country, branches/overseas subsidiaries of registered intermediaries are required to adopt the more stringent requirements of the two. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups shall be required to apply appropriate additional measures to manage the ML/TF risks, and inform SEBI.

3.2 OBLIGATION TO ESTABLISH POLICIES AND PROCEDURES

3.2.1 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 fulfillment of the aforementioned obligations.

a. “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.”

b. Financial groups shall be required to implement group wide programmes for dealing with ML/TF, which shall be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group as under:

I. policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

II. the provision, at group level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This shall include information and analysis of transactions or activities which appear unusual (if such analysis was done); similar provisions for receipt of such information by branches and subsidiaries from these group level functions when relevant and appropriate to risk management; and

III. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

3.2.2 To be in compliance with these obligations, the senior management shall be 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. We shall:

a. 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;

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

c. 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;

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

e. 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;

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

g. develop staff members' awareness and vigilance to guard against ML and TF.

3.2.3 Policies and procedures to combat ML and TF shall cover:

a. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities 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.

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.

The purpose of this document is to guide all the employees of **AAA Institutional Securities Private Limited** and employees of its associates on the steps that they are required to take and implement to prevent and identify any money laundering or terrorist financing activities. It shall be the responsibility of each of the concerned employees that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the “Prevention of Money Laundering Act, 2002”.

Some of these suggested measures may not be applicable to every circumstance or to each department, Branch / Sub-broker. However, each entity should consider carefully the specific nature of its business, type of customer and transaction to satisfy itself that the measures taken by the employees are adequate and appropriate to follow the spirit of these guidelines.

4. IMPLEMENTATION OF THIS POLICY

CLIENT DUE DELIGENCE

The CDD measures comprise the following:

The main aspect of this policy is the Customer Due Diligence Process which means:

a. To obtain sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

b. To verify the customer's identity using reliable, independent source document, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person. Provided that in case of a Trust, the reporting entity shall ensure that trustees disclose their status at the time of commencement of an account based relationship.

c. To identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted; The beneficial owner shall be determined as under:

✓where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation: For the purpose of this sub-clause:

i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;

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

✓ where the client is a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership

of/entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation: For the purpose of this clause:

"Control" shall include the right to control the management or policy decision;

✓ where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of such association or body of individuals;

✓ where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

✓ **For client which is a trust**: the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

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

✓ Applicability for foreign investors: Registered intermediaries dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client;

✓ The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset

Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

d. To verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and

e. To understand the ownership and control structure of the client.

f. To conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;

g. To review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data;

h. Registered intermediaries shall periodically basis and at least once a year update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.

i. To register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

j. Suspicious transactions relating to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIUIND."

✓ No transaction or account-based relationship shall be undertaken without following the CDD procedure."

5. CLIENT ACCEPTANCE POLICY

Client acceptance policies and procedures aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF. To apply client due diligence on a risk sensitive basis depends on the type of client business relationship or transaction. The following safeguards shall be followed by the company while accepting the clients:

- No account opened of or keeping any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

- Factors of risk perception (in terms of monitoring suspicious transactions) of the client shall be defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.

- Undertaking enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

NRIs, HNIs, Trust, Charities, NGOs, Organization receiving donation, Politically Exposed Persons (PEP) shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. The additional norms applicable to PEP as contained in paragraph 6 of the Circular shall also be applied to the accounts of the family members or close relatives of PEPs, persons of foreign origin, companies having closed shareholding/ownership, companies dealing in foreign currency, shell companies, overseas entities, non-face to face clients, and clients with dubious background.

Current/Former Head of State, Current/Former senior high profile politician, Companies offering foreign exchange, etc.) or clients from high-risk countries, i.e. while dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, while dealing with clients in high risk countries other than FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), we shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas;

- Documentation requirements and other information to be collected in respect of different classes of clients shall depend on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

- To ensure that an account is not opened where the company is unable to apply appropriate CDD measures/KYC policies. It shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non-genuine, or there is perceived non-co-operation of the client in providing full and complete information. In such a case, the company shall continue to do business with such a person and file a suspicious activity report. The company shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. A cautious step shall be taken to ensure that we do not return securities of money that may be from suspicious trades. The Company shall consult the relevant authorities in determining what action shall be taken when suspicious trading is suspected.

- The circumstances under which the client is permitted to act on behalf of another person/entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further

the rights and responsibilities of both the persons i.e. the agent-client registered with the intermediary, 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.

- Do not accept clients with identity matching with a person known to have criminal background: To check whether the client's identity matches with any person known to be having criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/regulatory agency worldwide.

6. CLIENT IDENTIFICATION PROCEDURE

The procedure shall include:

a. To put in place appropriate risk management systems to determine whether the client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.

b. Senior management approval shall be obtained 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, senior management approval to be obtained to continue the business relationship.

c. Reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

d. The client shall be identified by using reliable sources including documents/information. Adequate information shall be obtained to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

e. Adequate information shall be kept so as to satisfy competent authorities (regulatory/enforcement authorities) in future that due diligence was observed by the company in compliance with these directives. Each original document shall be seen prior to acceptance of

a copy.

f. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority/Senior Management.

An ongoing due diligence shall be conducted where inconsistencies in the information provided by the client has been identified. The underlying objective shall be to follow the requirements preserved in the PMLA, SEBI Act and Regulations, directives and circulars issued, so as to be aware of the clients on whose behalf the company is dealing.

It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available from obtaining the minimum information/documents from clients as stipulated in the PML Rules/SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/category-wise exemption available for carrying out CDD measures.

7. RELIANCE ON THIRD PARTY FOR CARRYING OUT CLIENT DUE DILIGENCE

Reliance may be placed 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 PML Act.

Such reliance shall be subject to conditions that are specified in Rule 9(2) of the PML Rules and further in line with the regulations and circular/guidelines as may be issued by SEBI from time to time. In terms of Rule 9(2) of PML Rules:

a) The registered intermediary shall immediately obtain necessary information of such client due diligence carried out by the third party;

b) The registered intermediary 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;

c) The registered intermediary 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 Act;

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

8. RISK-BASED APPROACH

a) Risk Based Approach (RBA) will be applied for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, same will be monitored on the implementation of the controls and enhance them if necessary.

b) It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, each of the clients due diligence measures on a risk sensitive basis shall be applied. The basic principle preserved in this approach is that an enhanced client due diligence process shall be adopted for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that shall be obtained necessarily would depend on the risk category of a particular client.

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

RISK ASSESSMENT

- Risk assessment to be carried out to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

- The risk assessment carried out shall also consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required by them.

- We shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products.

- We shall ensure: To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and Adoption of a risk based approach to manage and mitigate the risks".

- 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.

Risk Profiling of the Client

We at **AAA Institutional Securities Private Limited** accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as Low risk, medium risk and high risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client we have to apply higher degree of due diligence. The factors of risk perception depend on client's location, nature of business activity, turnover, nature of transaction, manner of payment etc. At **AAA Institutional Securities Private Limited** at the time of assessing risk profile of client we consider family background and credit worthiness of whole family as we as client annual income and Networth.

In order to achieve this objective, all clients of the branch should be classified in the following category:

¬ Category A – Low Risk
¬ Category B – Medium Risk
¬ Category C – High Risk

Factors of risk perception of the client:

Particulars	Factor of Bifurcation	Risk Category
Client of Special Categories & Non–resident (NRI)	Client`s Location	High Risk
Payment through Banker`s Cheque / Demand Draft / Cash / Chq of other bank (own) not mapped	Manner of Making Payment	Medium Risk
Client Introduced by other Existing Clients	Client`s Location	Low Risk
Client introduced through existing business network, Social circle/past known clients and Direct Clients	Client`s Location	Low Risk
Professional persons like Doctors, Lawyers, CA/CS/ICWAI/Engineers Etc	Nature of Business Activity, Turnover etc	Low Risk
Face to Face persons	Client`s Location	Low Risk
Face to Face clients of other than Region / Govt.	Client`s Location	Low Risk

/Defense Sector Employees		
Regular payment through A/c payee cheque from the Bank A/c already mapped with us	Manner of Making Payment	Low Risk

Ensure that no account is opened where we unable to apply appropriate clients due diligence measures/KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client or information provided by the client is suspected to be non genuine or perceived non-co-operation of the client in providing full and complete information. We should not continue to do business with such a person and file a suspicious activity report. We should also evaluate whether there is suspicious trading in the account and whether there is a need to freeze or close the account.

9. MONITORING OF TRANSACTIONS

Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that it can identify deviations in transactions/activities.

Special attention shall be paid to all complex unusually large transactions/patterns which appear to have no economic purpose. Internal threshold limits for each class of client accounts shall be defined and special attention shall be paid to transactions which exceeds these limits.

The background including all documents/office records/memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/stock exchanges/FIUIND/other relevant Authorities, during audit, inspection or as and when required.

Client due diligence measures shall also applied to existing clients on the basis of materiality and risk, and due diligence will be conducted on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

Record of the transactions in terms of Section 12 of the PMLA shall be preserved and those transactions of a suspicious nature or any other transactions notified under Section 12 of the Act shall be reported to the Director, FIU-IND. Suspicious transactions shall be regularly reported to the Senior Management.

10. SUSPICIOUS TRANSACTION MONITORING AND REPORTING

All are requested to analyze and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

What is a Suspicious Transaction?

- Clients whose identity verification seems difficult or clients appear not to cooperate;
- Substantial increase in activity without any apparent cause;
- Large number of accounts having common parameters such as common partners/directors/promoters/address/email address/telephone numbers/introducers or authorized signatories;
- Transactions with no apparent economic or business rationale;
- Sudden activity in dormant accounts;
- Source of funds are doubtful or inconsistency in payment pattern;
- Unusual and large cash deposits made by an individual or business;
- Transfer of investment proceeds to apparently unrelated third parties;
- Multiple transactions of value just below the threshold limit of Rs.10 Lacs specified in PMLA so as to avoid possible reporting;
- Clients transferring large sums of money to or from overseas locations with instructions

for payment in cash;

- Purchases made on own account transferred to a third party through off market transactions through DP Accounts;
- Suspicious off market transactions;
- Large deals at prices away from the market;
- Accounts used as 'pass through'. Where no transfer of ownership of securities or trading is occurring in the account and the account is being used only for funds transfers/layering purposes;
- All transactions involving receipts by non-profit organizations of value more than rupees ten lakhs, or its equivalent in foreign currency;
- 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, as 'Clients of Special Category'. Such clients should also be subject to appropriate counter measures. These measures may 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.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, file STR if we have reasonable grounds to believe that the transactions involve proceeds of crime."

What to Report?

- Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer, Compliance Officer, Principal Officer or any other designated officer.
- The notification may be done in the form of a detailed report with specific reference to

the clients, transactions and the nature/reason of suspicion.

- The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature/reason of suspicion.
- In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.
- The Principal Officer/Money Laundering Control 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.
- It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents.
- It is clarified that intermediaries should report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

11. INFORMATION TO BE MAINTAINED

Following information in respect of transactions referred to in Rule 3 of PML Rules shall be maintained:

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.

12. RECORD KEEPING REQUIREMENTS & RETENTION OF RECORDS

Records pertaining to transactions of clients shall be maintained and preserved for a period of **Eight years** from the date of the transaction. Record of documents evidencing the identity of the clients and beneficial owners (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence shall be maintained and preserved for a period of **five years** even after the business relationship with the client has ended or the account has been closed, whichever is later.

Records shall be maintained 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 or if there be any suspected drug related or other 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 this reconstruction, the following information of the client shall be maintained in order to maintain a satisfactory audit trail:

a. the beneficial owner of the account;

b. the volume of the funds flowing through the account; and

c. for selected transactions:

i. the origin of the funds;

ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.;

iii. the identity of the person undertaking the transaction;

iv. the destination of the funds;

v. the form of instruction and authority.

System is been maintained to record all such transaction as prescribed under Rule 3 of the PML Rules as follows:

a. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

b. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

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

c. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

d. 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.

Where there is no have of the identity of its existing clients, the records shall obtain forthwith, failing to which we shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules.

Record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, shall be maintained and preserved for a period of five years from the date of the transaction with the client.

In the case of transactions where any investigations by any authority has been commenced and in the case of transactions which have been the subject of suspicious transactions reporting all the records shall be maintained till the authority informs closure of the case.

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

In terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, 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, Government of India has outlined a procedure through an order dated February 02, 2021 for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021. A corrigendum dated March 15, 2023 has also been issued in this regard. The list of Nodal Officers for UAPA is available on the website of MHA.

14. 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

I. 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.

II. 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.

(3) 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."

III. The stock exchanges and registered intermediaries are directed to comply with the procedure laid down in the said Order.

IV. The stock exchanges and registered intermediaries shall:

(a) Maintain the list of individuals/entities ("Designated List") and update it, without delay, in terms of paragraph 2.1 of the Order;

(b) 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, stock exchanges and registered intermediaries 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

(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, stock exchanges and registered intermediaries 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) send a copy of the communication, mentioned in paragraphs III(ii) and IV(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;

(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 covering all transactions in the accounts, covered under paragraphs IV(ii) and (iii) above, carried through or attempted through.

V. 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.

VI. Reporting entities shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

15. LIST OF DESIGNATED INDIVIDUALS OR 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'. We 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 http://www.un.org/sc/committees/1267/consolist.shtml.

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

Precaution shall be taken to ensure that no account is opened whose name shall be appearing in such list. Periodic review of the existing account shall be conducted to ensure that no existing account is linked to any of the entity or individual included in the list. Any resemblance found shall be reported to SEBI and FIU-IND.

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

We 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.

We 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.

16. 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 the registered intermediaries.

We 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 from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

17. REPORTING TO FIU

In terms of the PMLA rules, brokers and sub-brokers are 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

Reporting of cash and suspicious transactions as per the schedule given below:

AAA INSTITUTIONAL SECURITIES PVT LTD

Space On B-16-A, Plot No-5, Community Centre, New Friends Colony, New Delhi - 110065 | Tel. No.: 011 - 49948719 | Mob. No. +91-96677 38861

Email: info@aaa-securities.com | Website: www.aaa-securities.com

CIN: U66120DL2026PTC464792

Report	Description	Due Date
CTR	All cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency	15th day of the succeeding month
CTR	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 have taken place within a month	15th day of the succeeding month
STR	All suspicious transactions whether or not being made in cash	Not later than seven days on satisfied that the transaction is suspicious
NTR	Non-Profit Organization Transaction Report	15th day of the succeeding month

The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND. Utmost confidentiality shall be maintained in filing of 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.

“Non-profit organization” means any entity or organization, 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);”

We DP, its Directors, officers and all employees 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.

There shall not be any restrictions on operations in the accounts where an STR has been made. The DP and the directors, officers and employees (permanent and temporary) will be 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.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in the PMLA, 2002, an STR shall be filed, if there is reasonable grounds to believe that the transactions involve proceeds of crime.

18. PRINCIPAL OFFICER

The Principal Officer 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 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.

In terms of Rule 2(f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by a registered intermediary; Provided that such officer shall be an officer at the management level.

19. DESIGNATED DIRECTOR

"Designated Director" means a person designated by the Board of Directors to ensure overall

compliance with the obligations imposed under The Prevention of Money Laundering Act, 2002 and the Rules framed there under, as amended from time to time, and include the Managing Director or a Whole-time Director duly authorized by the Board of Directors.

The Company shall appoint a Designated Director and communicate the details of the Designated Director, such as name, designation and address to the Office of the Director, FIU-IND and update the same whenever there is any change.

20. DETAILS OF DESIGNATED DIRECTOR & PRINCIPAL OFFICER

Particulars	DESIGNATED DIRECTOR	PRINCIPAL OFFICER
Name	MAYANK SHARMA	_____
Designation	DESIGNATED DIRECTOR	PRINCIPAL OFFICER
Office Address	SPACEON B-16-A, PLOT N-5, COMM. CENTRE, SRINIWASPURI, SOUTH DELHI, DELHI, INDIA-110065	_____
Telephone Number	+91-9667738861	_____
Email ID	compliance@aaa-securities.com	_____

21. SYSTEM AND PROCEDURE FOR HIRING OF EMPLOYEES

i. The Department Heads shall be involved in hiring of new employees, shall adequately carry out the screening procedure in place to ensure high standards in hiring new employees.

ii. Bona fides of employees are checked to ensure that the employees do not have any link with terrorist or other anti-social organizations.

iii. Reference of candidate: - Candidate having reference would be called for the interview. In case of employee having applied through newspaper would be called for the interview after scrutinizing his/her bio-data.

iv. Background of the candidate: - Background of the employee should be clean & under no circumstances candidate who has left earlier employer due to dispute should be selected.

v. Third party verification of candidate: - If necessary third party verification should be done by making phone call.

vi. Experience: - Candidate should have to appear for the skilled test depending on the exposure.

vii. Candidate should be aware for PMLA 2002 guidelines. Proper training should be given if he/she is not aware.

22. EMPLOYEES TRAINING

- Importance of PMLA Act & its requirement to employees through training.
- Ensuring that all the operating and management staff fully understands their responsibilities under PMLA for strict adherence to customer due diligence requirements from establishment of new accounts to transaction monitoring and reporting suspicious transactions to the FIU.
- Organizing suitable training programmes wherever required for new staff, front-line staff, supervisory staff, etc.
- Briefings to new employees at induction programs and rounds of small meetings and presentations at branch locations.
- Adequate training should be given to all the concerned employees to (a) ensure that the

contents of the guidelines are understood and (b) develop awareness and vigilance to guard against money laundering and terrorist financing.

- As of now, AML policy will be covered during the induction training given to all new recruits and also during the on-going compliance sessions.

23. INVESTORS EDUCATION

As the implementation of AML/CFT measures being sensitive subject and requires us to demand and collect certain information from investors which may be of personal in nature or has hitherto never been called for, which information include documents evidencing source of funds/income tax returns/bank records etc. and can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information.

There is, therefore, a need for us to sensitize the clients about these requirements, as the ones emanating from AML and CFT framework. We shall circulate the PMLA Circulars and other specific literature/pamphlets etc. so as to educate the client of the objectives of the AML/CFT program. The same shall also be emphasized on, in the Investor Awareness Programs conducted by us at frequent intervals of time. The importance of the same is also made known to them at the time of opening the Account.

POLICY REVIEW AND APPROVAL

Note: This policy has been reviewed in terms of SEBI's circular HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023, vide Circular No. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated June 16, 2023 and SEBI's circular SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06, 2024 by Board of Directors of **AAA Institutional Securities Private Limited** during its meeting held on **26th October 2026** and is being circulated to all concerned for compliance of the same.

Above Policy will be Reviewed once in every one year or as per regulatory requirements.