PMLA / ANTI-MONEY LAUNDERING POLICY

Clearmind Consultancy Private Limited
SEBI Registered Research Analyst
SEBI Registration No.: INH000025179

1. INTRODUCTION

Clearmind Consultancy Private Limited ("Clearmind" / "the Company"), a SEBI registered Research Analyst bearing Registration Number INH000025179, is committed to complying with the applicable provisions of the Prevention of Money Laundering Act, 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Rules"), applicable SEBI regulations, circulars, guidelines and directions, and other applicable laws relating to prevention of money laundering and combating the financing of terrorism ("AML/CFT").

This Policy establishes the framework and procedures to be followed by Clearmind to prevent its services, systems, personnel and business relationships from being used, intentionally or unintentionally, for money laundering, terrorist financing or other financial crimes.

The Policy is applicable to the Company, its directors, employees, officers and other personnel involved in client onboarding, client servicing, compliance, operations, research and related activities, to the extent applicable.

2. OBJECTIVES OF THE POLICY

1. To prevent Clearmind from being used, intentionally or unintentionally, for money laundering, terrorist financing or other illicit financial activities.
2. To establish appropriate standards for Know Your Client (KYC) and Client Due Diligence (CDD).
3. To verify and establish the identity of clients and, where applicable, their beneficial owners.
4. To understand the nature and purpose of the client relationship and, where appropriate, the source of funds and source of wealth.
5. To adopt a risk-based approach for identification, assessment and monitoring of clients.
6. To identify and monitor unusual or suspicious transactions and activities.
7. To maintain adequate records and documents to enable reconstruction of transactions and provide an audit trail.
8. To report suspicious transactions and other reportable transactions to the Financial Intelligence Unit – India (FIU-IND), wherever required under applicable law.
9. To ensure that Clearmind does not establish or continue relationships with persons or entities where applicable legal, regulatory or sanctions requirements prohibit such relationships.
10. To ensure appropriate employee awareness and training regarding AML/CFT requirements.

3. SCOPE AND APPLICABILITY

This Policy shall apply to the Board of Directors of Clearmind; Principal Officer and Designated Director; Compliance Officer; employees and other personnel involved in client-facing or compliance-related functions; all clients and prospective clients of Clearmind; and transactions and activities undertaken in connection with the services provided by Clearmind.

The Policy shall be read together with the applicable provisions of PMLA, PML Rules, SEBI regulations, SEBI circulars/directions and other applicable statutory or regulatory requirements.

Where there is any change in applicable law or regulatory requirements, the applicable statutory/regulatory requirement shall prevail over any inconsistent provision of this Policy.

4. GOVERNANCE AND RESPONSIBILITY

Clearmind shall maintain an appropriate internal framework for implementation of AML/CFT requirements.

The following persons shall be responsible for the overall implementation and supervision of this Policy:

Name: Mr. Punam Kucheria
Designation: Principal Officer & Designated Director

Name: Mrs. Deepa Kucheria
Designation: Compliance Officer

Contact Details:
Email: admin@iamclearmind.com
Phone: +91 9372810916

The Principal Officer shall act as the central point of reference for AML/CFT matters and shall coordinate with the relevant regulatory/statutory authorities wherever required.

5. CLIENT DUE DILIGENCE (CDD) AND KYC

Clearmind shall undertake appropriate CDD/KYC measures before establishing a client relationship and at such other times as may be required under applicable laws and regulations.

The CDD process shall, as applicable, include:
1. Obtaining and verifying prescribed KYC documents and information.
2. Identifying and verifying the identity of the client.
3. Obtaining information regarding the nature and purpose of the proposed relationship.
4. Identifying the beneficial owner, wherever applicable.
5. Obtaining additional information or documents where the client is assessed as higher risk.
6. Conducting appropriate screening against applicable sanctions and watch lists.
7. Conducting periodic review and updating of client information based on the client's risk classification.
8. Maintaining appropriate records of the KYC/CDD process.

Clearmind may seek additional documents or information where the information provided by a client is insufficient, inconsistent, outdated or raises reasonable concerns.

6. CLIENT ACCEPTANCE POLICY

Clearmind shall ensure that:
1. No client relationship shall be established in a fictitious, anonymous or false name.
2. Clearmind shall not establish or continue a client relationship where it is unable to complete the applicable CDD/KYC requirements.
3. Where information provided by a client is suspected to be false, misleading or non-genuine, the client relationship shall not be established or may be subject to appropriate restrictions or termination.
4. Clearmind shall not knowingly establish or continue a relationship where doing so would violate applicable sanctions, regulatory or legal requirements.
5. Appropriate measures shall be taken where the identity of the client, beneficial owner or other relevant person matches or potentially matches an applicable sanctions/watch list.
6. The Company shall assess the risk associated with each client and classify clients based on applicable risk factors.
7. Higher-risk clients shall be subject to enhanced due diligence and enhanced monitoring, wherever required.

7. RISK CLASSIFICATION

Clearmind shall adopt a risk-based approach for classification of clients.

Clients may generally be classified as:
• Low Risk
• Medium Risk
• High Risk

Risk assessment may take into consideration factors including, but not limited to:
• Client type and legal structure;
• Nature of business or occupation;
• Geographic location;
• Country/jurisdiction of residence or incorporation;
• Beneficial ownership structure;
• Nature and expected level of transactions;
• Source of funds and source of wealth, where applicable;
• PEP status;
• Sanctions/watch-list status;
• Non-face-to-face relationship;
• Adverse information available from reliable public sources; and
• Any other factor relevant to the AML/CFT risk assessment.

The risk classification shall be reviewed periodically and whenever there is a material change in the client's circumstances or risk profile.

8. ENHANCED DUE DILIGENCE

Enhanced Due Diligence ("EDD") shall be undertaken for clients or situations presenting higher AML/CFT risks, wherever applicable.

Such measures may include:
• Obtaining additional identification documents;
• Establishing the source of funds and/or source of wealth;
• Obtaining additional information regarding the nature and purpose of the relationship;
• Obtaining additional information regarding beneficial ownership;
• Conducting enhanced screening and verification;
• Obtaining appropriate senior-level approval for establishing or continuing the relationship; and
• Increasing the frequency and extent of transaction monitoring.

9. POLITICALLY EXPOSED PERSONS (PEPs)

Clearmind shall take appropriate measures in relation to clients who are identified as Politically Exposed Persons ("PEPs"), their family members and/or close associates, as applicable under prevailing laws and regulations.

Appropriate enhanced due diligence and monitoring shall be undertaken as required by applicable regulatory requirements.

Where required, appropriate approval shall be obtained before establishing or continuing the relationship with such clients.

10. SANCTIONS AND SCREENING

Clearmind shall undertake appropriate screening of clients and, where applicable, beneficial owners against relevant sanctions lists and other applicable regulatory/watch lists.

Particular attention shall be given to applicable lists issued or notified by competent authorities, including relevant United Nations Security Council sanctions and lists prescribed by Indian authorities.

Where a potential match is identified, the Company shall undertake appropriate verification and escalation before proceeding with or continuing the relationship.

Any confirmed match shall be dealt with strictly in accordance with applicable law and regulatory requirements.

11. SUSPICIOUS TRANSACTIONS AND ACTIVITIES

Clearmind shall maintain procedures to identify transactions or activities that may give rise to suspicion of money laundering, terrorist financing or other unlawful activity.

Indicators that may require enhanced scrutiny include, but are not limited to:
1. Difficulty in verifying the identity of the client.
2. Client unwillingness to provide required KYC/CDD information or supporting documents.
3. Information that appears inconsistent, false or unverifiable.
4. Transactions or activities that do not appear to have a reasonable economic or lawful purpose.
5. Unusual or complex transactions inconsistent with the client's known profile.
6. Significant or unusual changes in the nature or volume of activity without reasonable explanation.
7. Unexplained third-party payments or transfers.
8. Transactions involving high-risk jurisdictions where appropriate controls are considered inadequate.
9. Attempts to structure transactions to avoid applicable reporting or monitoring thresholds.
10. Any other activity which, based on the facts and circumstances, gives reasonable grounds for suspicion.

12. REPORTING OF SUSPICIOUS TRANSACTIONS

Where a transaction or activity is identified as suspicious, the Principal Officer shall evaluate the matter and take appropriate action in accordance with applicable law.

Where required under PMLA/PML Rules and applicable regulatory requirements, the Company shall file a Suspicious Transaction Report (“STR”) with FIU-IND within the prescribed time and manner.

Attempted transactions may also require reporting where prescribed under applicable law, even if the transaction was not completed.

The fact of filing an STR, or information relating to an STR, shall be kept confidential and shall not be disclosed to the concerned client or any unauthorized person, except where disclosure is permitted or required by law.

13. TRANSACTION MONITORING

Clearmind shall undertake monitoring appropriate to the nature, size and risk profile of its business and client relationships.

Particular attention shall be given to:
- Unusually large or complex transactions;
- Transactions that have no apparent economic or lawful purpose;
- Transactions inconsistent with the client's known profile;
- Unusual patterns of activity;
- Transactions involving high-risk jurisdictions;
- Transactions involving third parties without a reasonable explanation;

• Repeated attempts to conduct transactions that raise AML/CFT concerns; and
• Transactions or activities that otherwise warrant enhanced scrutiny.

The Company shall maintain appropriate records of the review, investigation and conclusions relating to identified unusual or suspicious activity.

14. CASH TRANSACTIONS

Clearmind shall comply with applicable legal and regulatory requirements concerning cash transactions and reporting of cash transactions.

The Company shall not knowingly accept cash payments where such acceptance is prohibited under applicable law, regulatory requirements or internal policies.

Where any reportable cash transaction or connected series of cash transactions falls within the applicable reporting requirements under PMLA/PML Rules, the same shall be appropriately recorded and reported to FIU-IND within the prescribed time and manner.

15. RECORD KEEPING AND RETENTION

Clearmind shall maintain records as required under applicable provisions of PMLA, PML Rules, SEBI regulations and other applicable laws.

Records shall be maintained in a manner that enables the Company and competent authorities to:
• Reconstruct individual transactions;
• Establish the identity of the parties involved;
• Identify the nature, amount and date of transactions;
• Identify the beneficial owner, wherever applicable;
• Establish the source and destination of funds, wherever applicable; and
• Provide an appropriate audit trail.

Records relating to transactions and client identification shall be retained for the period prescribed under applicable law.

Where records relate to ongoing investigations, proceedings or transactions that have been reported as suspicious, such records shall be retained for the period required under applicable law or until the relevant matter is concluded, as applicable.

16. INFORMATION TO BE MAINTAINED

Where applicable, records shall contain sufficient information regarding:
1. Nature of the transaction;
2. Amount and currency of the transaction;
3. Date of the transaction;
4. Parties involved in the transaction;
5. Beneficial owner;
6. Source and destination of funds, wherever applicable;
7. Relevant account or client details;
8. Supporting documents; and
9. Any other information required under applicable law.

17. REPORTING TO FIU-IND

Clearmind shall comply with applicable reporting requirements to the Financial Intelligence Unit – India (FIU-IND).

The Company shall report such information as may be required under PMLA, PML Rules and applicable regulatory requirements, including, where applicable:
• Suspicious Transaction Reports (STRs);
• Cash Transaction Reports (CTRs); and
• Other prescribed reports.

Reports shall be submitted through the prescribed FIU-IND reporting mechanism within the applicable timelines.

FIU-IND:
Financial Intelligence Unit – India
Department of Revenue, Ministry of Finance
Government of India
Website: fiuindia.gov.in

18. PRINCIPAL OFFICER

The Principal Officer shall be responsible for overall coordination and implementation of the AML/CFT framework of Clearmind.

The Principal Officer shall, as applicable:
1. Have access to relevant client identification and CDD information.
2. Ensure effective implementation of this Policy.
3. Review and evaluate potentially suspicious transactions and activities.
4. Ensure timely reporting of applicable transactions to FIU-IND.
5. Maintain appropriate confidentiality regarding STRs and related information.
6. Ensure that relevant records and information are made available to competent authorities when lawfully required.
7. Respond promptly to requests from SEBI, FIU-IND and other statutory/regulatory authorities.
8. Ensure appropriate AML/CFT training and awareness among relevant employees.
9. Monitor changes in applicable PMLA, PML Rules, SEBI and other regulatory requirements.
10. Escalate material AML/CFT issues to the appropriate management/Board level, wherever necessary.

19. DESIGNATED DIRECTOR

The Designated Director shall oversee the overall compliance framework relating to AML/CFT requirements and ensure that the Company maintains appropriate systems and procedures for compliance with applicable PMLA and PML Rules.

The Designated Director shall:
• Ensure that adequate AML/CFT policies and procedures are established;
• Ensure appropriate allocation of responsibility for AML/CFT compliance;
• Oversee implementation of the Policy;
• Ensure that appropriate records are maintained;
• Support the Principal Officer in discharging statutory responsibilities; and
• Take appropriate corrective measures where deficiencies in AML/CFT compliance are identified.

Designated Director: Mr. Punam Kucheria

20. COMPLIANCE OFFICER

The Compliance Officer shall assist in ensuring compliance with applicable AML/CFT requirements and shall coordinate with the Principal Officer and relevant personnel.

The Compliance Officer shall, as applicable:
• Assist in implementation of KYC/CDD procedures;
• Monitor compliance with internal AML/CFT procedures;
• Assist in periodic client review;
• Escalate unusual or potentially suspicious activity;
• Maintain relevant compliance records;
• Assist in regulatory inspections and audits; and
• Monitor regulatory developments relevant to AML/CFT compliance.

Compliance Officer: Mrs. Deepa Kucheria

21. EMPLOYEE SCREENING AND TRAINING

Clearmind shall maintain appropriate employee screening procedures, commensurate with the nature of the employee's role and responsibilities.

Relevant employees shall receive appropriate AML/CFT training and awareness covering:
• KYC and CDD requirements;
• Client risk classification;
• Identification of suspicious activities;
• Escalation procedures;
• Record keeping requirements;
• Confidentiality requirements;
• PMLA/PML Rules requirements; and
• Changes in applicable regulatory requirements.

Training shall be conducted periodically and whenever material changes in AML/CFT requirements warrant such training.

22. CONFIDENTIALITY AND NON-DISCLOSURE

All information relating to suspicious transaction identification, internal investigation and reporting shall be treated as confidential.

No employee or representative of Clearmind shall disclose to a client or any unauthorized person that:
• An STR has been filed;
• A suspicious transaction is under review; or
• Information relating to a suspicious transaction has been provided to a competent authority,
except where such disclosure is expressly permitted or required by law.

23. INTERNAL CONTROLS AND PERIODIC REVIEW

Clearmind shall maintain appropriate internal controls to ensure effective implementation of this Policy.

The Company shall periodically review:
• Client KYC/CDD records;
• Risk classifications;
• Applicable sanctions/watch lists;
• Transaction monitoring procedures;

• AML/CFT controls;
• Employee training requirements; and
• Compliance with applicable reporting obligations.

Any material deficiencies identified shall be appropriately escalated and corrective measures shall be implemented.

24. AUDIT, INSPECTION AND REGULATORY COOPERATION

Clearmind shall maintain adequate records and documentation to demonstrate compliance with applicable AML/CFT requirements.

Such records shall be made available to SEBI, FIU-IND, auditors, law enforcement agencies or other competent authorities whenever lawfully required.

The Company shall provide appropriate cooperation and timely responses to regulatory or statutory requests for information.

25. POLICY REVIEW AND AMENDMENT

This Policy shall be reviewed periodically and whenever there is a material change in:
• PMLA or PML Rules;
• SEBI regulations, circulars or directions;
• FIU-IND reporting requirements;
• Applicable sanctions requirements; or
• The nature or scope of Clearmind's business.

Necessary amendments shall be made to ensure continued compliance with applicable legal and regulatory requirements.

The amended Policy shall be placed before the appropriate authority of the Company for approval, wherever required.