ANTI MONEY LAUNDERING (AML) POLICY

1. Background, Scope and Objective

Background

The Prevention of Money Laundering Act, 2002 ("PMLA") came into force on 1 July 2005, and the Rules under it were notified on the same date by the Department of Revenue, Ministry of Finance, Government of India. Under the PMLA, every banking company, financial institution and intermediary, including an investment adviser registered under Section 12 of the Securities and Exchange Board of India Act, 1992 ("SEBI Act"), must follow client identification procedures, maintain records of transactions as prescribed, and report specified transactions to the Financial Intelligence Unit – India ("FIU-IND").

Scope

This Policy applies to **JMD Aarthiq Private Limited** along with its group entities (the "Company"), to all directors and employees, and to every client and service of the Company. It is framed under the PMLA, the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ("PML Rules"), the SEBI Master Circular on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) dated 6 June 2024 as amended from time to time, the SEBI (Investment Advisers) Regulations, 2013 and the circulars issued under them, and the recommendations of the Financial Action Task Force ("FATF").

Responsibility of the Company

The Company is fully committed to comply with all applicable laws designed to combat money laundering and any activity which facilitates the funding of terrorist or criminal activities. This Policy will be amended from time to time as required by SEBI, FIU-IND or any other competent authority, and in line with FATF requirements.

Objectives

1. To lay down the AML/CFT Policy of the Company.
2. To ensure that the Company and its clients are not vulnerable to money laundering and that the Company is not used as a conduit for it.
3. To ensure compliance with AML laws and regulations in force from time to time.
4. To protect the Company's reputation.
5. To assist law enforcement agencies in their efforts to investigate and track money launderers.
6. To lay down AML compliance norms for the employees of the Company.

JMD Aarthiq Private Limited
SEBI Registration No: INA000023302
CIN: U82990BR2026PTC081813
Registered Office: Plot No. 60, Nandan Puri, Maurya Path, B V College, Phuylwari, Patna-800014
Corporate Office: Ground Floor, A-46/1, Naraina Vihar, New Delhi-110028

2. Definitions

- **Client** means any person who engages, or seeks to engage, the Company for investment advisory services, including a prospective client during onboarding.
- **Beneficial Owner** means the natural person(s) who ultimately own or control a client, or on whose behalf a transaction is conducted, identified using the ownership and control thresholds prescribed in the PML Rules and the SEBI AML Master Circular.
- **Clients of Special Category (CSC)** include non-resident clients, high net worth clients, trusts, charities and non-governmental organizations, companies with close family shareholdings or complex ownership, politically exposed persons, clients from high-risk jurisdictions, and clients not met in person.
- **Politically Exposed Person (PEP)** means an individual who is or has been entrusted with a prominent public function, together with their family members and close relatives, as defined in the PML Rules and SEBI circulars.
- **Designated Director** means the person designated by the Board to ensure overall compliance with the obligations under Chapter IV of the PMLA and the PML Rules.
- **Principal Officer** means the officer designated by the Company to report to FIU-IND and to implement this, Policy.
- **Employee** means every director, officer, permanent or temporary employee, and any person associated with investment advice or client servicing.

3. Money Laundering – Definition and Stages

Money laundering is moving illegally acquired money through financial systems so that it appears to be legally acquired. There are three common stages, which launderers use and which institutions may unwittingly be exposed to while undertaking normal business:

1. **Placement** – the physical disposal of cash proceeds derived from illegal activity.
2. **Layering** – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and
3. **Integration** – creating the impression of apparent legitimacy for criminally derived wealth, by placing the laundered proceeds back into the economy so that they re-enter the financial system as normal business funds.

Section 3 of the PMLA makes it an offence to directly or indirectly attempt to indulge in, knowingly assist, be a party to, or be actually involved in any process or activity connected with

the proceeds of crime, including its concealment, possession, acquisition or use, and to project or claim it as untainted property.

4. Money Laundering Risks

The Company is exposed to the following risks if an appropriate AML framework is not established:

1. **Reputation Risk** – risk of loss due to severe impact on the Company's business, which requires maintaining the confidence of regulators, clients, creditors and the general marketplace.
2. **Compliance Risk** – risk of loss due to failure to comply with key regulations governing the Company's operations.
3. **Operations Risk** – risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.
4. **Legal Risk** – risk of loss due to any of the above resulting in failure to comply with law, including fines, confiscation of proceeds of crime, suspension or cancellation of registration by regulators, and criminal liability.
5. **Financial Risk** – risk of loss due to any of the above resulting in a negative financial impact on the Company.

5. Governance: Board, Designated Director and Principal Officer

5.1 Board

The Board of Directors approves this Policy, reviews its operation at least annually, and ensures that the Designated Director and the Principal Officer have the authority, independence and resources needed to perform their roles.

5.2 Designated Director

The Board designates Mayank Prakash as Designated Director. The Designated Director ensures overall compliance with the obligations imposed under Chapter IV of the PMLA and the PML Rules, and the Company intimates the appointment, and any change, to FIU-IND and SEBI as required.

5.3 Principal Officer

The Board designates Mayank Prakash as Principal Officer. The Principal Officer has timely access to client identification data, KYC information, transaction records and other relevant information, and:

- implements this Policy effectively and monitors compliance by Employees;

- registers the Company as a reporting entity with FIU-IND and files STRs and other reports within the prescribed timelines;
- records the reasons for treating, or not treating, any transaction as suspicious;
- ensures that Employees are trained and have the resources to apply this Policy to specific facts;
- acts as the point of contact for FIU-IND, SEBI and law enforcement agencies; and
- reports to the Board at least annually on the operation of this Policy, alerts raised, reports filed and training done.

6. Client Acceptance and Risk Categorization

6.1 Client acceptance

- No account will be opened in an anonymous, fictitious or benami name, or where the client's identity cannot be established.
- The Company will not onboard a client, or will end the relationship, where client due diligence cannot be completed, where the client gives false or misleading information, or where the client's identity matches a person with a known criminal background, a banned entity, or a person or entity linked to terrorists or terrorist organizations.
- Where a prospective client is refused, the Principal Officer assesses whether an STR must be filed.

6.2 Risk Categorization

Each client is assigned a risk category (low, medium or high) at onboarding, based on the client's nature and type, occupation and source of funds, geography, ownership structure, mode of onboarding and the services sought. The category is reviewed at each periodic review and on any trigger event. Clients of Special Category are treated as high risk unless the Principal Officer records a reasoned decision otherwise.

6.3 Enhanced due diligence

For high-risk clients and Clients of Special Category, the Company will:

- obtain senior management approval before onboarding a PEP, or before continuing the relationship where an existing client becomes a PEP;
- establish the source of funds and, where relevant, the source of wealth, with supporting documents;
- carry out more frequent reviews and closer monitoring; and

- register non-profit organization clients on the DARPAN portal of NITI Aayog and keep those records for five years, as the SEBI AML Master Circular requires.

7. Client Due Diligence (KYC)

7.1 Basic due diligence

Having regard to the guidelines of SEBI and other regulators and to the risk that financial services may be used by money launderers, the Company makes reasonable efforts to establish the real identity of every client by proper Client Due Diligence (CDD). Procedures obtain the information needed to identify each new client, using the KYC Registration Agency (KRA) and CKYCR systems as SEBI permits, and verify it from original or officially valid documents. The client's PAN, address, contact details, financial situation and the purpose and intended nature of the relationship are recorded.

7.2 Beneficial ownership

For clients that are not individuals, the Company identifies and takes reasonable steps to verify the natural persons who ultimately own or control the client, using the thresholds prescribed in the PML Rules and the SEBI AML Master Circular. Where no natural person can be identified, the senior managing official is treated as the beneficial owner.

7.3 When CDD is carried out

1. **New clients:** KYC and CDD are completed before any agreement are entered into or any advisory service is provided.
2. **Ongoing basis:** Client information is reviewed periodically, and whenever additional investments or fee remittances are inconsistent with the client's known profile, the client's information changes, or there is doubt about the accuracy of earlier information.
3. **Reliance on third parties:** The Company may rely on a KRA, CKYCR or another regulated third party for CDD, but remains responsible for the outcome.

Clients are required to keep their contact details, including email and mobile number, updated with the Company at all times.

8. Payments and Handling of Funds

- Advisory fees are accepted only by account payee cheque, demand draft or electronic transfer (NEFT, RTGS, IMPS or UPI) from the client's own bank account, as the SEBI Master Circular for Investment Advisers requires. The Company does not accept cash.
- Payments from third parties are not accepted. Any refund is made only to the account from which the payment was received.

- The Company does not accept funds from clients for investment, does not hold client securities, and never asks for a client's login credentials, passwords or OTPs for trading, demat or bank accounts.
- Any attempt by a client to pay in cash, or through a third party, is treated as an alert and referred to the Principal Officer.

9. Monitoring and Suspicious Transaction Reporting

9.1 Ongoing monitoring

Special attention is given to complex, unusually large transactions and unusual patterns that have no apparent economic or visible lawful purpose. Employees and the customer service team must report to the Principal Officer any behavior of a client that appears suspicious at the time of interaction. Indicative alerts include:

- reluctance to provide information or documents, or documents that appear false or altered;
- fees or investments inconsistent with the client's known income, occupation or profile;
- payments from accounts not belonging to the client, or attempts to pay in cash;
- transactions structured to avoid reporting or monitoring, or sudden changes in behavior;
- links to sanctioned or high-risk jurisdictions, or to persons with adverse media; and
- unusual interest in secrecy, or in the Company's reporting obligations.

9.2 Escalation and reporting

- An Employee who forms a suspicion must report it to the Principal Officer immediately, in writing, giving the client, the transaction and the grounds for suspicion.
- The Principal Officer evaluates the report, records the reasons for the decision, and where the transaction or attempted transaction is suspicious files a Suspicious Transaction Report (STR) with FIU-IND on the FINnet portal within the timeline prescribed by SEBI and FIU-IND. Suspicious attempted transactions are reported even if they were not completed.
- Cash Transaction Reports (CTR), Counterfeit Currency Reports (CCR) and Non-Profit Organization Transaction Reports (NTR) are filed as and when applicable. As the Company does not accept cash, a CTR is not expected, but any cash received in breach of this Policy is reported.

9.3 Prohibition on "tipping off"

Employees (permanent and temporary) must maintain strict confidentiality and must not disclose to the client or to any other person that an STR or related information has been, or is being, reported to FIU-IND. Employees who report in good faith are protected from retaliation.

10. Sanctions and List Screening

- Clients are screened against the lists of individuals and entities designated under UN Security Council Resolutions, the orders issued under section 51A of the Unlawful Activities (Prevention) Act, 1967 ("UAPA") and section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, and other lists notified by SEBI or the Government of India.
- Screening is carried out at onboarding and again each time the lists are updated, and covers existing clients, beneficial owners and, where relevant, connected parties.
- On receipt of an order to freeze or unfreeze under section 51A of the UAPA, the Company implements it without prior notice to the designated individuals or entities and reports as prescribed. Any matching record is reported to the relevant authority.
- Particular care is taken with clients, and funds, connected to jurisdictions that FATF identifies as high-risk or under increased monitoring.

11. Record Keeping

The Company maintains records, in electronic or paper form, of the nature, value and date of transactions and the parties to them, of the identity-verification documents, of STRs and other reports filed, and of records of client interactions. These records are sufficient to permit the reconstruction of individual transactions, so as to provide evidence for prosecution of criminal activity if necessary.

Records are retained for at least five years after the end of the business relationship, or for any longer period that other laws require. Where an investigation, inquiry or dispute is pending, records are kept until it concludes. The Principal Officer, the Designated Director and staff assisting them have timely access to identification data and records, which are available promptly to competent authorities.

12. Hiring, Training and Investor Education

12.1 Hiring

The Company has adequate screening procedures when hiring Employees and monitors the selection process. Any unfair practice reported is investigated and acted on.

12.2 Training

- **New Employees** who deal with clients or their transactions receive a general introduction to money laundering and to identifying and reporting suspicious transactions, regardless of seniority.
- **Client-facing staff** are the first point of contact with potential money launderers and must be made aware of this Policy, and of the extra vigilance needed for non-regular clients and large transactions.
- **Ongoing training** is refreshed at least annually and covers AML definitions, guidelines and requirements; risks of non-compliance; prevention of fraud and suspicious transactions; and mandatory documentation.
- Records of training are maintained.

12.3 Investor education

Clients are informed, when onboarded, why the Company asks for identity, financial and source-of-funds information under AML laws, and that this is a regulatory requirement.

13. Internal Control, Audit and Group-wide Application

- The Company verifies on a regular basis compliance with the policies, procedures and controls relating to money laundering. An independent review of the AML function is carried out at least annually by internal audit or an external reviewer, and exceptions are reported to the Board, or its Audit Committee if one has been constituted.
- Where the Company has group entities, this Policy applies on a group basis, and information is shared within the group for AML and CFT purposes subject to applicable law and client confidentiality.

14. Review of the Policy

This Policy will be reviewed at least annually, and whenever a law, rule or SEBI or FIU-IND circular changes. Changes arising from experience and from regulatory change will be incorporated and approved by the Board.