



KERALA INFRASTRUCTURE FUND MANAGEMENT LIMITED

ANTI-MONEY LAUNDERING POLICY

JUNE 2023

Policy	Anti-money laundering policy	Version: 1.0
<p>Reference:</p> <p>KIFML :</p>		<p>Effective date:</p> <p>Approved by:</p>

Revision History

Base Version	Release date	Rationale for change	Summary of changes	Updated by	Approved by
1.0					
1.1					
1.2					

1. PREAMBLE

The prevention of Money Laundering Act, 2002 (PMLA) enacted in 2003 came into force with effect from 1st July 2005 to prevent money laundering and to provide for attachment, seizure and confiscation of property obtained or derived, directly or indirectly, from or involved in money laundering and for matters connected therewith or incidental thereto. Necessary Notifications/Rules under the said Act were published in the Gazette of India on July 01, 2005.

Pursuant to the recommendations made the Financial Action Task Force (FATF) on anti- money laundering standards, SEBI has issued a master circular No. CIR/ISD/AML/3/2010 dated December 31, 2010 on anti-money laundering/ Combating the Financing of Terrorism (CFT) in line with the FATF recommendations and PMLA Act, 2002. As per the Guidelines on Anti Money Laundering standards notified by SEBI, all registered intermediaries have been advised to ensure that proper policy frameworks are put in place.

2. BACKGROUND AND OBJECTIVES

The objective of the policy is to ensure that we identify and discourage any money laundering or terrorist financing activities and that the measures taken by the Company are adequate to follow the word and spirit of the Act and guidelines. As per the provisions of the PMLA, Intermediary includes a stockbroker, sub-broker, share transfer Agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with the Securities market and registered under section 12 of the Securities and Exchange Board of India Act,1992(SEBI Act).

The Company shall put in place proper systems and processes to ensure that the Funds managed by it adheres to client account opening procedures and maintain records of such transactions as prescribed by the PMLA and Rules notified there under. And strictly follow the necessary SEBI directives and circulars from time to time, covering issues related to Know your Client (KYC) norms, Anti-Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT). The directives issued by SEBI so far lay down the minimum requirements and emphasize that the intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

This Anti Money Laundering (AML) Policy requires the employees with considerable knowledge of the working of the company to recognize questionable financial transactions, and to take steps to conduct appropriate additional due diligence. If any 'Red Flag', whether or not listed in this AML Policy is triggered, the employees need to promptly contact the Company's Compliance Officer to facilitate any further due diligence or action that may be needed. The Company is also committed to cooperate with law enforcement and regulatory agencies enforcing anti-money laundering laws and regulations.

This Policy defines a minimum standard. However, when applicable anti-money laundering laws are stricter than this policy, such laws must be complied with. In case of any doubts, employees must contact our Company's Compliance Officer.

This policy should be supplemented by the Whistle-blower Policy, the Anti-Bribery and Anti-Corruption Policy, any guidance published pursuant to this policy, and any other relevant policies as may be implemented from time to time.

3. DEFINITION OF MONEY LAUNDERING

- 3.1. Section 3 of the Prevention of Money Laundering (PML) Act 2002 defines the "Offence of money laundering" as under: "Whosoever directly or indirectly attempts to indulge or knowingly assist or knowingly is party or is actually involved in any process or activity connected with the proceeds of crime, including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering"
- 3.2. The term 'proceeds of crime' has been defined under Section 2(u) of the PMLA as "any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property."
- 3.3. Money launderers use the Financial Intermediaries/Banking System for cleansing 'dirty money' obtained from criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions to hide the origin and true nature of the funds.
- 3.4. The term 'money laundering' would also cover Financial Transactions where the end use of funds goes for terrorist financing.

4. IDENTIFYING MONEY LAUNDERING

Money laundering usually consists of 3 (three) steps:

- 4.1. **Placement:** This is the initial stage and during this stage, the money generated from illegal/criminal activity such as sale of drugs, illegal firearms, etc. is disposed of. Funds are deposited into financial institutions or converted into negotiable instruments such as money orders or traveller's cheques. For example, cash received by a drug smuggler can be taken to a bank and changed into a money order or traveller's cheque.
- 4.2. **Layering:** In this stage, funds are moved into other accounts in an effort to hide their origin and separate illegally obtained assets or funds from their original source. This is achieved by creating layers of transactions, by moving the illicit funds between accounts, between businesses, and by buying and selling assets on a local and international basis until the original source of the money is virtually untraceable. Thus, a trail of unusually complex transactions is created to disguise the original source of funds and thereby make it appear legitimate. For example, money can be moved into and out of various offshore bank accounts through electronic funds transfers.

- 4.3. **Integration:** Once the illegitimate money is successfully integrated into the financial system, these illicit funds are reintroduced into the economy and financial system and often used to purchase legitimate assets, fund legitimate businesses, or conduct other criminal activity. The transactions are made in such a manner so as to appear as being made out of legitimate funds.

5. PREVENTION OF MONEY LAUNDERING ACT, 2002

Section 12 of PML Act 2002 places certain obligations on every Financial Institution/Intermediary/ Banking company which include:

- 5.1. Maintaining a record of prescribed transactions
- 5.2. Furnishing information of prescribed transactions to the specified Authority
- 5.3. Verifying and maintaining records of the identity of the investors/customers
- 5.4. Preserving records in respect of (i), (ii), (iii) above for a period of 10 years from the date of cessation of transactions i.e. the date of termination of account or business relationship between the client/ investor and the intermediary.

6. POLICY OBJECTIVES

- 6.1. To prevent criminal elements from using the System for money laundering activities.
- 6.2. To enable the Company as an intermediary to keep track of the financial transactions of the investors in the Funds managed by it.
- 6.3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- 6.4. To take necessary assistance from RTA in complying with applicable laws and regulatory guidelines.
- 6.5. To take necessary steps to ensure that the concerned staff members are adequately trained in KYC/AML procedures.

7. Money Laundering – Risk Perception:

- 7.1. Money laundering activities expose the Intermediary / Financial Institution to various risks such as:
- a. **Reputation Risk:** Risk of loss due to severe impact on the reputation of the Financial Institution/Intermediary. This would be a matter of concern given the nature of business in Alternate Investment Fund (AIF) industry, which requires the confidence of investors.
 - b. **Compliance Risk:** Risk of loss due to failure of compliance with key regulations governing the AIF activities.
 - c. **Operational Risk:** Risk of loss resulting from inadequate or failed Internal Processes, People and Systems or from external events.
 - d. **Legal Risk:** Risk of loss due to any legal action, the RTA / Investment Manager or its staff may face due to failure to comply with the law.

8. Scope:

This policy is applicable to all Funds managed by KIFML & their activities and should be read in conjunction with related Operational Guidelines/Regulations issued by SEBI for Investment Manager from time to time.

This AML Policy is applicable to all individuals working at all levels and grades associated with the Company who has access to undisclosed information and such other persons including those designated by the Compliance Officer from time to time.

9. Implementation of Anti Money Laundering Activities at KIFML:

- 9.1. The Company Secretary cum Compliance Officer is presently appointed as the Principal Officer by KIFML, for the Funds managed by them, to comply with the SEBI Anti Money Laundering Guidelines, 2006. The Principal Officer will define / implement appropriate criterion for identifying the Suspicious Transactions and reporting of the same to Financial Intelligence Unit (FIU), New Delhi. The contact details of the Principal Officer will be communicated to FIU, New Delhi.
- 9.2. If required, the Board of the Company also may appoint a Designated Director to ensure overall compliance of AML/CFT
- 9.3. The main objective of this policy is the Client Due Diligence Process (CDD) which means:
 - a. Obtaining sufficient information about the client / customer/investor to identify who is the actual beneficial owner of the securities or on whose behalf transaction is made.
 - b. Verify the customer's/investor's identity using reliable, independent source, document, data or information.
 - c. Conduct on-going due diligence and scrutiny of the account/client to ensure that the transaction conducted are consistent with the client's background/financial status, its activities and risk profile
- 9.4. **Customer Due Diligence** (in accordance with SEBI Anti Money Laundering Guidelines, 2006 and all amendments thereafter). This Process involve Five specific parameters:
 - a. Policy for Acceptance of Clients/Customers/Investors
 - b. Suspicious Transactions identification & reporting
 - c. Risk Based Approach
 - d. Clients of special category (CSC)
 - e. Client Identification procedure.

Integrated Registry Management Services Private Limited (Integrated) acts as the 'Registrar & Transfer Agent (RTA)' to the Investment Manager, KIFML. The relationship between the KIFML and Integrated is that of 'Principal & Agent'. The customers/investors are procured by KIFML.

Integrated Registry Management Services Private Limited, as an R & T Agent does not have any role to play in the same. However, they perform a supportive role in providing the required information to KIFML. Hence, the responsibility of applying the KYC procedures, as required under the Prevention of Money Laundering Act and SEBI Guidelines, primarily lies with KIFML. SEBI has prescribed certain KYC norms as a matter of reference to all the Funds regulated by them.

9.5. **New KYC Norms:** Effective January 1, 2011 KYC compliance was made mandatory for all categories of investors irrespective of the amount invested. SEBI has introduced usage of uniform KYC by all SEBI registered intermediaries. SEBI, vide a gazette notification dated 2nd December-2011, notified SEBI {KYC(Know Your Client) REGISTRATION AGENCY} REGULATIONS, 2011. Apart from carrying out the KYC, it is mandatory for intermediaries to carry out In- Person verification (IPV) of all its new investors.

9.6. **Due Diligence Norms for Foreign Investors** (SEBI Circular for foreign investment in Alternate Investment Fund, SEBI/HO/AFD-1/PoD/P/CIR/2022/171)

The following shall be ensured by the fund at the time of onboarding a foreign investor:

- Foreign investor of the AIF is a resident of the country whose securities market regulator is a signatory to the International Organization of Securities Commission's Multilateral Memorandum of Understanding or a signatory to the bilateral Memorandum of Understanding with SEBI.
- AIFs may accept commitment from an investor being Government or Government related investor, who does not meet the aforesaid condition, if the investor is a resident in the country as may be approved by the Government of India.
- The investor, or its underlying investors contributing twenty-five percent or more in the corpus of the investor or identified on the basis of control, is not the person(s) mentioned in the Sanctions List notified from time to time by the United Nations Security Council and is not a resident in the country identified in the public statement of Financial Action Task Force as:
 - a jurisdiction having a strategic Anti-Money Laundering or Combating the Financing of Terrorism deficiencies to which counter measures apply; or
 - a jurisdiction that has not made sufficient progress in addressing the deficiencies or has not committed to an action plan developed with the Financial Action Task Force to address the deficiencies.
- In case an investor who has been on-boarded to scheme of an AIF, subsequently does not meet the conditions specified above, the manager of the AIF shall not drawdown any further capital contribution from such investor for making investment, until the investor again meets the said conditions. The same shall also apply to investors already on-boarded to existing schemes of AIFs, who do not meet conditions specified above.

9.7. **Compliance Steps for Employees:**

Each Employee should ensure that he/she undertakes the following steps in the course of the business operations of KIFML:

- 9.7.1. **Know your business partners:** Where appropriate, Employees should conduct integrity assessments and other due diligence exercises and be familiar with business practices of customers and suppliers.
- 9.7.2. **Monitor financial activity:** Employees should observe and record payments and transactions consistent with all established policies and procedures and follow global financial standards for acceptable forms of payment.
- 9.7.3. **Keep complete records:** Employees should always keep current, complete and accurate records of every business transaction.

- 9.7.4. **Report any suspicious activity:** Each Employees has an obligation under this AML Policy to immediately report to the Compliance Officer any Suspicious Transaction (as defined below) or suspicious activity or 'Red Flag' concern. Each Employees shall be aware of and follow country legal requirements for the reporting of cash transactions.

9.8. Suspicious Transaction:

A "Suspicious Transaction" includes an attempted transaction, whether or not made in cash, which to a person acting in good faith:

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

9.9. Potential Red Flags:

An exhaustive list of Red Flags cannot be provided, however, indicative actions or situations or parties that Employees should be careful about are listed below:

- a. Customers or suppliers who are connected to countries identified as non-cooperative by the 'Financial Action Task Force on Money Laundering' established by the G-7 Summit in 1987, and international organisations against money laundering;
- b. Customers or suppliers who are reluctant to provide complete information and/or provide insufficient, false, or suspicious information or who are unwilling to comply with KIFML's KYC norms as may be in force from time to time;
- c. Customers or suppliers who appear to be acting as an agent for another company or individual, but decline or are reluctant to provide information regarding that company or individual;
- d. Customers or suppliers who express concern about, or want to avoid, reporting or record- keeping requirements;
- e. Cash payments in excess of Rs. 20,000/- (Rupees Twenty Thousand only) or made in cash equivalents, such as money orders, traveller's cheques, internet currencies or prepaid cash cards. Acceptance of such amounts of cash or cash equivalents as a form of payment by our Company is strongly discouraged. Employee should be particularly wary of customers and suppliers who structure these payments to avoid government reporting requirements for cash and cash equivalent payments (e.g.: making multiple smaller payments or payments from multiple sources);
- f. The purchase of products, or a larger volume purchase, that appears to be inconsistent with a customer's normal ordering pattern, and in the absence of any legitimate business reason such as a special price promotion
- g. Complex deal structures or payment patterns that reflect no real business purpose or economic sense
- h. Requests for payment to be made through an unrelated country or to an unrelated third party

- i. Multiple partial payments from various parties on behalf of a single customer and/or multiple partial payments from various locations.
- j. Customers or suppliers whose address is not a physical site
- k. Customers making a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose
- l. Customers paying in one form of payment and then requesting a refund of the payment in another form

10. Suspicious Transaction Monitoring & Reporting

- 10.1. Once an investor invests in any of the Funds managed by the Company, handled by Integrated, it is necessary to keep track of their transactions to ensure that they are not indulging in any of the activities prohibited under law. It is incumbent on the part of RTA to identify the Suspicious Transactions and report to KIFML/the Fund in the form of an STR (Suspicious Transaction Report) and if found necessary to FIU, New Delhi, through Investment Manager. For preparing STR, the RTA will carry out scrubbing of investor details with designated Sanction Lists like UNSC, OFAC, UKHMT, SEBI, CBI, SATP etc.
- 10.2. Though the primary responsibility of identifying suspicious transactions vests with the Investment Manager, as an R & T Agent and Record Keeper, Integrated must provide details sought by KIFML for proper compliance of AML Regulations.
- 10.3. The criterion for identifying the Suspicious Transactions is reviewed by FIU/SEBI/AMFI and Investment Manager from time to time to ensure the objective of Anti Money Laundering Act including the amendments thereto, if any, is achieved.
- 10.4. The Unit Manager at Integrated is responsible for incorporating necessary controls in the processing through Information Technology Team for extracting the data of Suspicious Transactions as per the criteria and provide the same to the Investment Manager in the approved format and within the timelines specified by FIU/IM.

11. Reporting of Suspicious Transaction

- 11.1. The transactions as per the specified criteria shall be reported to IM in the format prescribed by FIU. Once the IM identifies a transaction as suspicious, RTA must prepare a Suspicious Transaction Report in the FIU prescribed format and provide the same to the IM, for onward reporting to FIU, New Delhi.
- 11.2. The reporting is to be done as per the procedure and within the time specified in the rules mentioned in the PML Act, 2002 and/or the circulars issued by SEBI from time to time.
- 11.3. The Suspicious Transaction Report (STR) should be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or noncash, or a series of transaction integrally connected are of suspicious nature.
- 11.4. The Unit Manager at CAMS shall ensure that strict and uncompromising confidentiality is maintained in respect of the transactions reported to IM as per the criteria and no information shall

be passed on to the investor concerned unless specifically and expressly approved by IM. Any deviation in this regard shall be viewed against the concerned Unit Manager.

12. Consequences of Violation of AML Policy by Designated Persons

In case of violations of the AML Policy, the Compliance Officer shall, after considering inputs, if any, from the Designated Director have the discretion to do the following:

- 12.1. **Corrective Action:** If necessary, corrective actions shall be prescribed by the Compliance Officer to appropriate managers, officers, or other employees for implementation.
- 12.2. **Penalties:** The Compliance Officer shall, based on the investigation reports (if any) have the discretion to recommend appropriate disciplinary action, including suspension and termination of service, against such a defaulting Designated Person. Depending on the nature and scale of default of the AML Policy by the defaulting Designated Person, the Compliance Officer may also recommend to the Board to commence civil and/or criminal proceedings against such a Designated Person in order to enforce remedies available to our Company under applicable laws.

13. Maintenance of Records:

- 13.1 The Fund shall ensure that the records related to Suspicious Transactions are preserved and maintained, for a period of 10 (ten) years, from the date of transaction/reporting whichever is earlier.

The information that are to be maintained are:

1. nature of transaction
2. amount of transaction and the currency in which is denominated.
3. date on which the transaction was conducted
4. parties to the transaction

Besides, the RTA shall also maintain the following:

- a. The beneficial owner of the account
- b. The volume of the funds flowing through the account
- c. For selected transactions: - the origin of the funds - the form in which the funds were offered or withdrawn - the identity of the person undertaking the transaction - the destination of the funds - the form of instruction and authority.

14. Retention of Records:

- 14.1. The records mentioned in Rule 3 of PMLA Rules including the corresponding/relevant records must be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client/investor and the intermediary.

- 14.2. Records on customer identification (e.g., copies or records of official identification documents like passports, identity cards including PAN Cards, driving licenses or similar documents), account files and business correspondence should also be kept for the same period.
- 14.3. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be preserved for a period of ten years from the date of cessation of the transactions between the client/investor and the intermediary.

15. Review of the Policy& Training:

- 15.1. Principal Officer along with any other authority responsible for over-all monitoring of the level of compliance activities by KIFML and/or its group Companies shall review this policy as and when any changes/amendments take place either in the AML Act and/or the regulations issued by SEBI.
- 15.2. The Principal Officer shall ensure that adequate training is imparted to all the concerned Officers Handling R & T activities of Fund business so as to ensure that the contents of the guidelines are understood and to develop awareness and vigilance to guard against money laundering and terrorist financing.

Annexure 1: Check list for due diligence with respect to foreign investors

Sl. No.	Document Type	Yes	No
1.	Constitutive Documents (MoA, COI, prospectus, etc.)		
2.	Proof of Address (Power of Attorney having address provided to Custodian is accepted as address proof.)		
3.	PAN		
4.	Board Resolution (Power of Attorney granted to Global custodian/ local custodian is accepted in lieu of Board Resolution (BR).)		
5.	FATCA (Foreign Account Tax Compliance Act) / CRS form		
6.	KYC Form		
7.	List of Signatures (BR and the authorized signatory list (ASL) is not required if SWIFT is used as a medium of instruction)		
8.	List of Ultimate Beneficiary Owner (UBO) including the details of Intermediate BO. (UBO is not required for Government and Government related entities)		
9.	Proof of Identify		

End of document