



ANTI MONEY LAUNDERING POLICY

Objective	This Policy establishes guidelines so that Paradise Moon Investment Fund I ("The Fund") complies with the provisions of the Prevention of Money Laundering Act (PMLA), 2002. It ensures that the Fund adheres to client account opening procedures and maintaining records of such transactions as prescribed by the PMLA and rules notified there under.
Rationale & Scope	"Policy" or "This Policy" means, Anti Money Laundering Policy or Know Your Client Policy. The purpose of This Policy is to set the steps that the Fund shall implement to discourage and to identify any money laundering or terrorist financing activities.
Applicability	This Policy applies to the Fund and all the Fund(s) managed by the Fund.
Approved By	The Policy is approved by the Management of the Fund
Review History	This Policy is to be reviewed annually. It may be amended from time to time at the discretion of the Management.

THE POLICY
Framework of Policies and Procedures to Combat Money Laundering (ML) and Terrorist Financing (TF)
In accordance with the PMLA, the Fund is mandated to- <ul style="list-style-type: none">• Establish and regularly update stringent and holistic policies and procedures, for dealing with ML and TF, in accordance with the current statutory and regulatory requirements.• Establish Client acceptance policies and procedures by undertaking thorough Client Due Diligence (CDD) measures.• Ensure employee training for identifying, monitoring and reporting the ML and TF transactions, as per the prescribed procedures.
Compliance Officer



For the purpose of This Policy, the Chief Financial Officer, Mr. Naveen Bansal shall be the Compliance Officer ("CO").

The responsibilities of the Compliance Officer include-

- Ensuring that the Fund properly discharges its obligations to report suspicious transactions to the authorities.
- To act as a central reference point in facilitating onward reporting of suspicious transactions.
- To play an active role in the identification and assessment of potentially suspicious transactions

In addition to the appointment of a Compliance Officer, the Senior Partners of the Fund shall act as the Designated Directors for the purpose of This Policy.

The responsibility of the Designated Directors is to aid and supervise the Compliance Officer with respect to establishing, maintain, updating and reporting of the the Fund's Anti-Money Laundering Policy.

Client Due Diligence (CDD)

Definition of Customer/Client	"Customer" - Know Your Customer (KYC) Directions, 2016 ("KYC Directions") issued by RBI on February 25, 2016 defines 'Customer' as a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the
--------------------------------------	---

	<p>transaction or activity, is acting.</p> <p>For the purpose of This Policy, a Customer or a Client is defined as:</p> <ul style="list-style-type: none">• Any person or entity that maintains or proposes to maintain an account and/or has a relationship with the Fund;• The Beneficial Owner on whose behalf the account is maintained;• Beneficiaries of transactions conducted by professional intermediaries, such as Stock brokers, Chartered Accountants, solicitors etc. as permitted under the law;• Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Fund; <p>Any person or entity with whom transaction amount exceeds INR 1,000,000/-</p>
CDD Measures	<p>To adopt the envisaged PMLA provisions, following CDD measures are to be followed:</p> <ul style="list-style-type: none">• Obtain sufficient information in order to identify the Client.• Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the natural person on whose behalf a transaction is being conducted• Verify the Client's identity using reliable, independent source documents, data and information• The Fund shall onboard a client by obtaining Officially valid documents ("OVD") as prescribed in Annexure 1



Guidelines for customer identification procedure	<ul style="list-style-type: none">• Please refer Annexure 2
Guidelines for acceptance of Clients	<ul style="list-style-type: none">• No account is opened in a fictitious or anonymous name.• Ensure that an account is not opened where the CDD measures and KYC documentation cannot be implemented. Required checks and balance shall be put into place before opening an account to ensure that the identity of the Client does not match with any person having known criminal background or is debarred by RBI and SEBI in terms of criminal proceedings.• Specify the circumstances under which the Client is permitted to act on behalf of another person or entity. The Fund shall clearly lay down the manner in which an account shall be operated, transaction limits and authority matrix for an account.• The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism.
Risk Assessment	<ul style="list-style-type: none">• Categorise the Clients into low, medium and high risk to enable proper monitoring and risk management.• The categorisation is to be guided by nature of business, quantum of exposure and past dealings with them. Trusts, NGOs, Politically Exposed Persons (PEP), Non face to face customers, Companies having close family shareholding or beneficial ownership , firms with sleeping partners, individuals and entities on the watchlists, customers specifically identified by regulators, FIU ,Non-resident Clients from high-risk countries or with dubious reputation; could be classified under “High Risk” category by the management.• Documentation requirements and other information to be collected depending on the perceived risk and having regard to the requirements of Rule 9 of the PMLA Rules, Directives and Circulars issued by SEBI from time to time. The basic principle enshrined in this approach is to implement enhanced CDD higher risk categories of Clients. Conversely, a simplified CDD process may be adopted for lower risk categories of Clients.
Record Keeping	



- As dictated under Section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act), the Fund shall maintain a record of all the transactions including but not limited to-
 - All cash transactions of the value of more than INR 10 lakh or its equivalent in foreign currency.
 - All series of cash transactions integrally connected to each other and have taken place within a month, aggregating to value of more than INR 10 lakh or its equivalent in foreign currency.
 - All cash and non-cash suspicious transactions.
- The Fund shall maintain and preserve the following information
 - the beneficial owner of an account and/or the parties to the transaction;
 - the volume of the funds flowing through an account;
 - the nature of the transactions;
 - the date, amount and the currency of the transactions;
 - for selected transactions (with high-risk Clients) additional record keeping shall be observed. The origin and destination of the funds, the mode of transaction, the identity of the person undertaking the transaction shall be diligently obtained and recorded.
- The Fund shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data.
- The records shall be maintained and preserved for a minimum period of ten years from the date of transaction, after the business relationship has been ended, or the account has been closed, whichever is later. However, where required by an investigating authority (In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting), certain Client records need to be stored and may exceed the prescribed requirements period.

Monitoring and Reporting

- The Fund would carry out on-going due diligence ("ODD") with respect to the business relationship with every customer closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile and, wherever necessary, the source of funds. Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures.
- The Fund shall pay special attention to all complex, unusually large transactions and patterns which appear to have no economic purpose. It shall pay special attention to transactions which exceeds the prescribed limits as per its Authorization Matrix.
- The background and all the documents, office records, memorandums, clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and the findings shall be recorded in writing. Further, such findings and records along with the related documents shall be made available to auditors and other relevant authorities.
- The Compliance Officer shall randomly examine a selection of transactions for healthy and



robust monitoring.

- The nature of a suspicious transaction includes but is not limited to the following-
 - Clients whose identity verification seems difficult or Clients that appear non cooperative while providing the details for the same;
 - Clients with dubious source of the funds which is either unclear or not in keeping with their apparent business activity;
 - Clients based in high risk jurisdictions;
 - Clients insisting on cash transactions;
 - Clients transacting in funds from unidentified or non-circumstantial overseas locations or from unrelated third parties.

- Any suspicious transaction shall be immediately notified to the Compliance Officer or the Management. This reporting shall constitute specific reference to the Clients, transactions and the nature or reason of suspicion. It shall be ensured that the Client is not informed of the said reporting.

- An updated list of individuals and entities who are subject to various sanction measures such as freezing of assets and 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.

If the name of the customer entity/individuals appears on the 2 lists of individuals and entities, suspected of having terrorist links, no account shall be opened by The Fund. The details of the 2 lists are as given below:

“ISIL (Da’esh) & Al-Qaida Sanctions List”

<https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/1267.pdf>

“1988 Sanctions List”

<http://www.un.org/sc/committees/1988/list.shtml>

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

The Management shall ensure that accounts are not opened in the name of anyone whose name appears or bear in resemblance to the entities in the said list. It shall regularly monitor all its existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

- **However, the overarching principle for ODD is that the extent of ODD/monitoring would be aligned with the risk category of the customer.**

Financial Intelligence Unit (FIU), India



- In accordance to PMLA Rules, The Management is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND)
 - The Management shall carefully consider the reporting requirements and formats that are available on the website of FIU-IND under the section 'Obligation of Reporting Entity – Furnishing Information – Reporting Format'. These documents contain detailed directives on the compilation and manner of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents.
-
- The identity inter alia the name, designation and address of the Compliance Officer, including any changes therein shall be intimated to the Office of the Director-FIU.
 - The Management shall submit the following-
 - The Cash Transaction Report (CTR), wherever applicable, for each month by 15th of the succeeding month.
 - The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.
 - The Non-Profit Organization Transaction Reports (NTRs) , wherever applicable, for each month shall be submitted to FIU-IND by 15th of the succeeding month.
 - The Compliance Officer shall be responsible for timely and observing utmost confidentiality in submission of CTR, STR and NTR to FIU-IND, as the case may be.
 - The Compliance Officer should record his reasons for treating any transaction or a series of transactions as suspicious.
 - No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious/non – profit organization transactions to be reported.



Paradise Moon Private Limited

CIN: U66309HR2023PTC117619

Add: 508, Tower - 5, Pyramid Homes II, Sector - 86,
Narsinghpur, Gurgaon, Haryana - 122004

Tel: +91 9999308633, **Email:** contact@paradisemoon.in



Registered Office

508, Tower - 5, Pyramid Homes II, Sector - 86, Narsinghpur, Gurgaon, Haryana - 122004

Tel: +91 9999308633, **Email:** contact@paradisemoon.in