SKI CAPITAL SERVICES LIMITED
Website: www.skicapital.net **E-mail**: contact@skicapital.net
SEBI Regn. No: INZ000188835 / IN-DP-08-2015
NSDL DP ID: IN301508 / IN301959
CDSL DP ID: 12098500

POLICIES AND PROCEDURE FOR COMBATING MONEY LAUNDERING(ML) OR TERRORIST FINANCING(TF)

(Issued as per the requirements of the PMLA Act 2002)

Version number	Adoption date
8.0	01/06/2023

Applicable on SKI Group companies, primarily consisting of

SKI Capital Services Limited, SEBI Registered Intermediary (Broking/ DP), RTA, Merchant Banker, IRDA Registered Corporate Agent, Surya Kiran Investment and Capital Services Pvt Ltd, IRDA Registered Corporate Agent and AMFI Registered Mutual Fund Distributor.

In compliance with

The PMLA Act 2002 as modified and rules there of SEBI Circular and Directives

Group Policy

It is our policy to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Principal Officer

The Group has designated Shri Narinder Wadhwa as the Principal Officer and Mr. Manick Wadhwa as the Designated Director of SKI Capital Services Ltd with full responsibility for the Group's AML program.

The Group has provided the FIU with contact information for the Principal Officer and Designated Director.

Overview

The primary objective of this Policy is to safeguard SKI Capital Services Limited against risks associated with money laundering and terrorist financing activities. This involves:

- Regulatory Compliance: Ensuring complete adherence to all statutory and regulatory requirements as specified under the Prevention of Money Laundering Act, 2002, and the guidelines issued by the Securities and Exchange Board of India (SEBI).

- Customer Identification: Employing robust Know Your Customer (KYC) procedures to ensure that the organization is well-acquainted with the identity, social and financial standing of its clients.

- Risk Assessment and Management: Systematically identifying, assessing, and taking effective countermeasures against risks related to money laundering and terrorist financing.

- Transparency and Accountability: Implementing due diligence procedures and maintaining transparent records of all financial transactions to ensure full accountability and traceability.

- Monitoring and Reporting: Continuous monitoring of customer accounts and transactions to detect and report suspicious activities in a timely manner to the Financial Intelligence Unit (FIU).

- Employee Training: Training employees regularly to update them on new regulations, trends in money laundering and terrorist financing, and measures to identify and report suspicious activities.

- Periodic Review and Updates: Continually updating the policy to incorporate changes in legislation, regulations, or specific guidelines issued by relevant authorities.

Background

1. 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, 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.

2. 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.

3. 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.

Policies and Procedures to Combat Money Laundering and Terrorist Financing Essential Principles:

1. This policy has taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed Directives 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 and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.

2. 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.

Obligation to establish policies and procedures

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 registered intermediaries ensure the fulfilment of the aforementioned obligations.

2. To be in compliance with these obligations, the senior management of a registered intermediary 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. The registered intermediaries shall:

3. Policies and procedures to combat ML and TF covers:

- 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;
- Client acceptance policy and client due diligence measures, including requirements for proper identification;
- Maintenance of records;
- Compliance with relevant statutory and regulatory requirements;
- Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
- 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; and,
- 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.

Written Anti Money Laundering Procedures

Client Due Diligence (CDD)

Objective

The objective of CDD measures is to form a reasonable belief regarding the true identity of each client and beneficial owner associated with the securities account. This also extends to understanding the ownership and control structure of the client and performing ongoing scrutiny of transactions.

Core Elements of CDD Measures

1. *Identification of Beneficial Owners*
- Obtain sufficient information to identify persons who beneficially own or control the securities account.
- When securities are beneficially owned by a party other than the client, identify that party using client identification and verification procedures.
- Verification of Client Identity
- Verify the client's identity using reliable, independent source documents, data, or information.

2. *Identification of Ownership and Control*
- For clients other than individuals or trusts, identify the beneficial owners and take reasonable measures to verify their identity through specific ownership percentages and control mechanisms.
- For trusts, identify and verify the identity of the author of the trust, trustee, protector, and beneficiaries with 15% or more interest in the trust.
- Listed companies and their majority-owned subsidiaries are exempt from these identification requirements.

3. *Verification of Beneficial Ownership*
- Verify the identity of the beneficial owner and/or the person on whose behalf a transaction is being conducted.

4. *Understanding Ownership and Control*
- Understand the ownership and control structure of the client.

5. *Ongoing Due Diligence*
- Conduct ongoing scrutiny of transactions and accounts throughout the business relationship.

6. *Review and Re-verification*

- Review due diligence measures and re-verify the identity of clients when there are suspicions of money laundering or financing of terrorism activities.

7. *Periodic Updates*

- Periodically update all documents, data, or information collected under the CDD process.
  i). On an annual basis- at the beginning of the financial year
  ii) At the time of reactivation of inactive clients
- Compliance Monitoring
- The Stock Exchanges and Depositories shall monitor compliance through half-yearly internal audits.
- In the case of mutual funds, compliance will be monitored by the Boards of the Asset Management Companies and the Trustees.
- For other registered intermediaries, compliance will be monitored by their Board of Directors.

Policy for acceptance of clients

Objective

The objective of this policy is to establish guidelines for client acceptance that aim to identify clients posing higher-than-average risks of Money Laundering (ML) or Terror Financing (TF). This will enable SKI Capital Services Limited to apply client due diligence on a risk-sensitive basis.

Guidelines for Client Acceptance

1. *No Anonymous Accounts*

- No anonymous or fictitious accounts shall be opened or maintained. Accounts on behalf of persons whose identity has not been disclosed or cannot be verified are not permitted.

2. *2. Risk Assessment Factors*

- Clients will be classified into low, medium, and high-risk categories based on location, nature of business activity, trading turnover, and payment methods.

3. 3. Clients of Special *Category* (CSC)

- Enhanced due diligence will be undertaken for CSC, which includes:
- Non-resident clients
- High net-worth clients
- Trust, Charities, NGOs
- Companies with close family shareholdings
- Politically Exposed Persons (PEP)
- Clients in high-risk countries
- Non-face-to-face clients
- Clients with dubious public reputation

4. *Documentation* Requirements

- Documentation and information to be collected will depend on the perceived risk and will comply with Rule 9 of the PML Rules, as well as directives and circulars issued by SEBI.

5. *Non-Cooperation by Clients*

- An account will not be opened if appropriate CDD measures cannot be applied due to non-cooperation by the client or if the information provided is suspected to be non-genuine.

6. *Authorization* for Acting on Behalf of Another

- The circumstances under which a client is permitted to act on behalf of another person/entity will be clearly specified, including operational and transactional limits.

7. Criminal Background *Checks*

- Necessary checks will be in place to ensure that the client does not have a known criminal background or is not banned by any enforcement agency worldwide.

8. *Revisiting* CDD Process

- The CDD process will be revisited when there are suspicions of ML/TF.

Compliance and Monitoring

The policy guidelines are illustrative, and SKI Capital Services Limited will exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

Client identification procedure

1. The KYC policy shall clearly spell out the client identification procedure (CIP) to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

2. Registered intermediaries shall be in compliance with the following requirements while putting in place a CIP**:**
   - We shall put in place appropriate risk management systems to determine whether their 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.
   - We obtain senior management approval 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, registered intermediaries shall obtain senior management approval to continue the business relationship.
   - We take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
   - The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
   - The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
   - Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

3. SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by SEBI from time to time, all registered intermediaries shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.

4. We shall conduct ongoing due diligence where it notices inconsistencies in the information provided.
5. We shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients. It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to registered intermediaries (brokers, depository participants, AMCs etc.) 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 by registered intermediaries. This shall be strictly implemented by all registered intermediaries and non-compliance shall attract appropriate sanctions.

Reliance on third party for carrying out Client Due Diligence (CDD)

Objective

The objective of this section is to outline the criteria, conditions, and procedures for relying on third parties for the purpose of carrying out Client Due Diligence (CDD).

Guidelines for Reliance on Third Parties

1. *Client Identification Procedure (CIP)*

- The KYC policy will clearly specify the CIP to be followed at different stages of the intermediary-client relationship, during transactions, or when doubts arise about previously obtained client identification data.

2. *Compliance Requirements*

- Registered intermediaries shall adhere to specific requirements, including:
- Risk assessment of clients or potential clients being Politically Exposed Persons (PEP).
- Obtaining senior management approval for business relationships with PEPs.
- Verifying the sources of funds and wealth for PEPs.

3. *Internal Directives*

- Based on SEBI's minimum requirements and established practices, registered intermediaries shall frame internal directives for CIP.

4. *Ongoing Due Diligence*

- Continuous due diligence will be conducted, especially when inconsistencies in the provided information are noticed.

5. *Comprehensive CIP*

- A comprehensive CIP shall be formulated, adhering to PML Rules and SEBI Circulars, without any minimum investment threshold or category-wise exemption.

i. Conditions for Relying on Third Parties

ii. Due Diligence: Prior to establishing a relationship with a third party for CDD, thorough due diligence must be conducted to assess the reliability and effectiveness of the third party's KYC procedures.

iii. Written Agreement: A written agreement should be in place between SKI Capital Services Limited and the third party, outlining the responsibilities of each party.

iv. Data Integrity: Ensure that the third party can provide accurate and updated data, and that SKI Capital Services Limited has the right to access such data when needed.

v. Compliance Check: Ensure that the third party is in compliance with all regulatory requirements related to CDD and is subject to periodic audits.

vi. Accountability: Despite relying on a third party, the ultimate responsibility for CDD compliance remains with SKI Capital Services Limited.

vii. Data Security: The third party must adhere to stringent data security protocols to safeguard client information.

viii. Notification: Clients must be notified that their information may be accessed by or shared with a third party for CDD purposes.

Compliance and Monitoring

Failure to adhere to these guidelines will result in appropriate sanctions. All efforts should align with the underlying objective to comply with the PMLA, SEBI Act, regulations, directives, and circulars.

Risk Management

Risk-based Approach

1. We shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, the registered intermediaries shall monitor the implementation of the controls and enhance them if necessary.

2. 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, the registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process 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 registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

3. Further, low risk provisions shall not apply 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

1. We shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

2. The risk assessment carried out shall 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.

3. 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.

Monitoring of Transactions

1. 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.

2. The intermediary shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The intermediary may specify internal threshold limits for each class of client accounts and pay special attention 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

1. in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/stock exchanges/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required.

2. The registered intermediaries shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

3. The intermediary shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be
4. regularly reported to the higher authorities within the intermediary.

5. Further, the compliance cell of the intermediary shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

Suspicious Transaction Monitoring and Reporting

1. We shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, registered intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

2. A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

- Clients whose identity verification seems difficult or clients that appear not to cooperate;
- Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
- Clients based in high risk jurisdictions;
- Substantial increases in business without apparent cause;
- Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- Attempted transfer of investment proceeds to apparently unrelated third parties;
- Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

3. Any suspicious transaction shall be immediately notified to the **Designated/Principal Officer** within the intermediary. 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. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ 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 Designated/ Principal 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.

4. 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 registered intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction

5. SEBI categorizes 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 'CSC'.

Record Management
Information to be maintained

- the nature of the transactions;
- the amount of the transaction and the currency in which it is denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

Record Keeping

1. Registered intermediaries shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

2. Registered Intermediaries shall maintain such records 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 behaviour.

3. In case of any suspected 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, registered intermediaries shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:
   - the beneficial owner of the account;
   - the volume of the funds flowing through the account; and
   - for selected transactions:
     - the origin of the funds
     - the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
     - the identity of the person undertaking the transaction;
     - the destination of the funds;
     - the form of instruction and authority.

4. Registered Intermediaries shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there under PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

5. More specifically, we have put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:
   - all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;
   - 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.
   - 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;

- 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 by the registered intermediary.

Retention of Records

6. We 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 as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of Eight years from the date of transactions between the client and intermediary.

7. As stated in paragraph 13 and 14, We are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of Eight years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

8. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

9. We shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of Eight years from the date of the transaction between the client and the intermediary.

Employees Hiring

We have adequate screening procedures in place to ensure high standard when hiring employees. We have identified the key positions within the Company structure having regard to the risk of money laundering and terrorist financing and the size of our business. We shall ensure that the employees taking up such key positions are suitable and competent to perform their duties
The HR Department is instructed to verify the identity, cross check all the references, family background and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting.
The department should obtain the following documents:
1 Photographs
2 Proof of address
3 Identity proof
4 Proof of Educational Qualification
5 Proof of Bank Account Details

Training of staff/Employees

All the staff members involved in front office dealings, back office, KYC & Compliances, Risk Management or any kind of client dealings to be adequately trained in AML and CFT (Combating Financing of Terrorism) procedures. They should fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of our systems being misused by unscrupulous elements.

Accordingly, we have an ongoing employee-training programme (in-house as well as sending employees for attending of independent training workshops) so that the concerned staff are adequately trained in AML and CFT procedures. These training programs are conducted on periodic basis and each of the concerned staff is required to attend atleast 2 such training programs each year.

Further, the Principle Officer is authorized to ensure that all the concerned staff is well versed with latest modifications in the PMLA policy framework and is adequately sensitized to the risks of ML & TF.

Procedure for freezing of funds, financial assets or economic resources or related services

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 **(UAPA),** relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Act and amendment thereto. In terms of said regulations, we as an intermediary have to ensure that we 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 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2).

Reporting to Financial Intelligence Unit-India

In terms of the PML Rules, we 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

Designation of officers for ensuring compliance with provisions of PMLA

1. **Appointment of a Principal Officer: T**he 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. As a matter of principle, it is advisable that the 'Principal Officer' is of a sufficiently senior position and is able to discharge the functions with independence and authority.

   Complete Details of the Principle Officer are as given below:
   Name : NARINDER WADWHA
   Designation : MANAGING DIRECTOR
   Contact No : 9810008640
   Email : md@skicapita.net

2. **Appointment of a Designated Director**: In addition to the existing requirement of designation of a Principal Officer, we shall also designate a person as a 'Designated Director'.

   Complete Details of the Designated Director are as given below:
   Name : MANICK WADWHA
   Designation : DIRECTOR
   Contact No : 9910785149
   Email : manick@skicapita.net

Updation/Review of the policy

The policy shall be reviewed/ updated on an annual basis

Approved at the Board meeting of SKI Capital Services Limited held on July 12, 2025

For **SKI Capital Services Limited**

Sd/-
(Narinder Wadhwa)
Director
DIN-00787274