

**NJ INDIA INVEST PRIVATE LIMITED**  
**POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING**  
**pursuant to requirements of the PMLA Act 2002 and amendments thereof**

---

**1 Company Policy**

It is the policy of the Company 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.

**2 Designation of an officer for reporting of suspicious transactions:**

**2.1 Principal Officer Designation and Duties**

The Company has designated Mr. Janak J Patel, Manager-Audit, as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the Company's AML program. Mr. Janak J Patel is qualified by experience, knowledge and training. The duties of the Principal Officer will include monitoring the Company's compliance with AML obligations and overseeing communication and training for employees. The Principal Officer will also ensure that proper AML records are kept. When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND). The Company has provided the FIU with contact information for the Principal Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The Company will promptly notify FIU of any change to this information.

**2.2 Appointment of a Designated Director**

In addition to the Principal Officer, the Company has designated the following director as "Designated Director":

<b>Sr. No.</b>	<b>Name of Chairman/ Managing Director/ Designated Director</b>	<b>Designation</b>	<b>Address</b>	<b>Email ID</b>	<b>Mobile Number</b>	<b>Telephone</b>
1	Niraj R. Choksi	Jt.Managing Director	7/E, Anjan Salaka Apt, Parle Point, Surat- 395009, Gujarat.	neeraj@njgroup.in	9374543685	0261-3985911

### 3 **Committee Composition:**

The head of Compliance, Operations, Finance and Audit functions/departments are been appointed as Committee Members to form the AML Committee. The AML Committee shall meet as often as its members deem necessary to perform the duties and responsibilities but not less than once in a Quarter. The AML Committee Meeting Minutes shall be considered, approved and taken on record in the immediate next Board Meeting.

### 4 **Customer Identification and Verification**

#### 4.1 At the time of opening an account, the Company will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status as under:

<b>Constitution of Client</b>	<b>Proof of Identity</b>	<b>Proof of Address</b>	<b>Others</b>
Individual	PAN Card	Copy of Bank Statement, etc	N.A.
Company	PAN Card Certificate of incorporation Memorandum and Articles of Association Resolution of Board of Directors	As above	Proof of Identity of the Directors/Others authorized to trade on behalf of the Company
Partnership Firm	PAN Card Registration certificate Partnership deed	As above	Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Trust	PAN Card Registration certificate Trust deed	As above	Proof of Identity of the Trustees/ others authorized to trade on behalf of the trust
AOP/ BOI	PAN Card Resolution of the managing body Documents to collectively	As above	Proof of Identity of the Persons authorized to trade on behalf of the AOP/ BOI

	establish the legal existence of such an AOP/ BOI		
--	---	--	--

- 4.2** If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open the new account.
- 4.3** All PAN Cards received will be verified from the Income Tax/ NSDL website before the account is opened.
- 4.4** The Company will maintain records of all identification information for five years after the account has been closed.
- 4.5 Identification of Beneficial Owners:**

**4.5.1 For clients other than individuals or trusts:**

Where the client is a person *other than an individual or trust*, viz., company, partnership or unincorporated association/body of individuals, the Company will identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

- a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

- i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
  - ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
  - iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.
- b. In cases where there exists doubt under clause 3.5.1 (a) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

- c. Where no natural person is identified under clauses 3.5.1 (a) or 3.5.1 (b) above, the identity of the relevant natural person who holds the position of senior managing official.

#### **4.5.2 For client which is a trust:**

Where the client is a *trust*, the Company will identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

## **5 Client Due Diligence**

### **5.1 The CDD measures of the Company comprise the following:**

- Obtaining sufficient information in order to identify persons who beneficially own or control the securities account shall be done diligently. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party will be identified using client identification and verification procedures.
- The identity of the client or the beneficial owner shall be verified by scrutinising independent and reliable source documents or information to establish the correct identity of the client/owner at the time of account opening.
- Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are in consistent with the registered intermediary's (Company) knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

### **5.2 Policy for acceptance of clients:**

- No account will be opened in a fictitious / benami name or on an anonymous basis.
- In line with the risk-based approach, the type and amount of identification information and documents required will depend on the risk category of a particular client.
- Documentation requirement and other information will be collected in respect of different classes of clients depending on perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

- The Company will not open account where it is unable to apply appropriate CDD measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, or the information provided is suspected to be non-genuine, or there is perceived non-co-operation of the client in providing full and complete information. The Company will not continue to do business with such a person.
- Necessary checks and balance are put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

### **5.3 Risk-based Approach**

- Clients will be categorized as High/ Low/ Medium risk depending on circumstances such as the client's background, type of business relationship or transaction etc. The Company will adopt an enhanced client due diligence process for higher risk categories of clients.
- Conversely, a simplified client due diligence process will be adopted for lower risk categories of clients.

### **5.4 Risk Assessment**

- The Company 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. The risk assessment will 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.
- The risk assessment carried out will 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 will be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

## **5.5 Clients of special category (CSC)**

- **Such clients include the following:**

- i. Non resident clients
- ii. High net-worth clients,
- iii. Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations.
- iv. Companies having close family shareholdings or beneficial ownership.
- v. Politically Exposed Persons (PEP) Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
- vi. Companies offering foreign exchange earnings.
- vii. Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
- viii. Non face to face clients.
- ix. Clients with dubious reputation as per public information available etc.

As per the independent judgment of the Company any other set of clients can be added.

The Company has in place procedure to identify persons of special category and additional necessary documents shall be collected from them.

The Company has also put in place necessary procedures to determine whether their existing/potential client is a PEP or a family member of the PEP or a close relative of PEP. Such procedures would include seeking additional information from clients, accessing publicly available information etc.

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

- i The Company may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

- ii Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the Company will be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

## **6 Maintenance of records**

As a policy no cash transactions are entered into by the Company, however the Principal Officer will be responsible for the maintenance of records.

All suspicious transactions means a transaction that -

- gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

## **7 Information to be maintained:**

The records shall contain the following information:

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

## **8 Retention of Records**

- The Company has taken 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 will be maintained and preserved for a period of five years from the date of transactions between the client and the Company.
- The records on client identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence will be maintained and preserved for a period of five years after the business relationship between a client and the Company has ended or the account has been closed, whichever is later.

- In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they will be retained until it is confirmed that the case has been closed.
- **Records of information reported to the Director, Financial Intelligence Unit – India (FIU-IND):**

The Company shall maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the Company.

## **9 Monitoring of transactions**

- Regular monitoring of transactions will be done to have a proper understanding of the normal activity of the client so that it can identify deviations in transactions / activities and in a way ensure the effectiveness of the AML policy.
- Proper checks and controls shall be implemented to identify that the funds received from the client are from his registered bank account, high value transactions and any abnormal transaction based on the nature of the client or his financial status and take necessary actions to verify the legitimacy of the source of funds.
- The Company will pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The Company has specified 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 will also be examined carefully and findings will be recorded in writing. Further such findings, records and related documents will be made available to auditors and also to SEBI/stock exchanges/FIU-IND/other relevant Authorities, during audit, inspection or as and when required. These records will be maintained and preserved for a period of five years from the date of transaction between the client and the Company as is required under PMLA.
- The Company will ensure that a record of the transactions is preserved and maintained and that transactions of a suspicious nature or any other transactions notified are reported to the Director, FIU-IND. Suspicious transactions will also be regularly reported to the higher authorities within the Company.



- Further, the Compliance Cell of the Company will 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.
- The Company will be cautious to ensure that it does not return securities of money that may be from suspicious trades. However, the Company will consult the relevant authorities in determining what action it should take when it suspects suspicious trading.

## **10 Monitoring Accounts For Suspicious Activity**

The Company monitors the transactions manually, which are in its belief to be suspicious transactions in terms of AML Policies. The Company has in place Back Office software named “SmallOffice” hired from TSS Consultancy to ascertain and identify the transactions of unusual size, volume, pattern or type. For non-automated monitoring, the following kinds of activities are to be mentioned as Red Flags and reported to the Principal Officer.

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Company's policies relating to the deposit of cash.
- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

When a member of the Company detects any red flag, he or she will escalate the same to the Principal Officer for further investigation.

## **11 Reporting to FIU IND**

As FIU IND has made filing of STR Mandatory in online mode through its Portal <https://fiuindia.gov.in> or <https://finnet.gov.in> w.e.f. 20th October 2012, the Company has been registered as Reporting Entity and received the FIU ID and the login details.

### **11.1 For Cash Transaction Reporting**

- All dealing in Cash that require reporting to the FIU IND will be done in the CTR format and in the matter and at intervals as prescribed by the FIU IND. However, as mentioned earlier, the Company does not accept transactions in Cash.

## 11.2 For Suspicious Transactions Reporting

- The Company will make a note of Suspicious Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND as per the required deadlines. This will typically be in cases where the Company know, suspect, or have a reason to suspect.

## 11.3 The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any the transaction reporting requirement.

- the transaction is designed, whether through structuring or otherwise, to evade any requirements of PMLA Act and Rules framed thereof
- the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and the Company know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- the transaction involves the use of the Company to facilitate criminal activity.

The Company will not take its decision on whether to file a STR solely on whether the transaction falls above a set threshold. The Company will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

All STRs will be reported quarterly to the Board of Directors, with a clear reminder of the need to maintain the confidentiality of the STRs.

The Company will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PMLA Act and Rules thereof.

## 12 AML Record Keeping

### (a) STR Maintenance and Confidentiality

The Company will hold STRs and any supporting documentation confidential. The Company will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about the STR. The Company will refuse any requests for STR information and immediately tell FIU IND of any such request it receive. The Company will segregate STR filings and copies of supporting documentation from other Company books and records to avoid disclosing STR filings. The Company's Principal Officer will handle all requests or other requests for STRs.

(b) Responsibility for AML Records and STR Filing

Principal Officer will be responsible to ensure that AML records are maintained properly and that STRs are filed as required.

(c) Records Required

As part of its AML program, the Company will create and maintain STRs and CTRs and relevant documentation on customer identity and verification. The Company will maintain STRs and their accompanying documentation for at least five years.

**13 Hiring of Employees**

The Company has adequate screening procedures in place to ensure high standards when hiring employees. The Company identifies the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

**14 Training Programs**

The Company will develop ongoing employee training under the leadership of the Principal Officer. The Company's training will occur on at least on annual basis. It will be based on the Company's size, its customer base, and its resources.

The Company's training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the Company's compliance efforts and how to perform them; the Company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PMLA Act.

The Company will develop training in the Company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

The Company will review the operations to see if certain employees, such as those in compliance, information security, internal audit, and other relevant functions, require specialized additional training. The Company's written procedures will be updated to reflect any such changes.

## **15 Investor Education**

The Company has the policy of sensitizing the clients about these requirements as the ones emanating from AML and CFT framework. The Company will prepare specific literature pamphlets etc. so as to educate the client of the objectives of the AML/CFT Programme in order to implement the AML/CFT measures which requires the Company to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information.

## **16 Program to test AML Program**

### **a) Staffing:**

The testing of the Company's AML program will be performed by the Internal Audit Team of the Company.

### **b) Evaluation and Reporting:**

After the Auditors have completed the testing, the Auditor staff will report its findings to the Board of Directors. They will address each of the resulting recommendations.

## **17 Monitoring Employee Conduct and Accounts**

The Company will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. The Company will also review the AML performance of supervisors, as part of their annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors.

## **18 Confidential Reporting of AML Non-Compliance**

Employees will report any violations of the Company's AML compliance program to the Principal Officer, unless the violations implicate the Principal/Compliance Officer, in which case the employee shall report to the Chairman of the Board, Such reports will be confidential, and the employee will suffer no retaliation for making them.

## **19 The Company has framed the policy based on the overall directives of PMLA 2002 including amendments thereof and other applicable laws even beyond its applicability for the kind of activities being performed by the Company in the current framework. In future, the Company shall endeavor to ensure that implementation of all the applicable provisions are complied within reasonable time frame.**

## **20 Board of Directors Approval**

This Policy and Procedure shall be considered and reviewed by the Board in its Board Meeting with an annual frequency and as and when updations made, if any.

The Board has approved this AML program as reasonably designed to achieve and monitor the Company's ongoing compliance with the requirements of the PMLA and implementing regulations under it.

*The board hereby considers and approves the PMLA Policy and procedure duly amended on its Board meeting held on 30/06/2015*

**- BY MANAGEMENT ORDER**