Doc No:-SIPL/DOC/2596 **Date**:-05th April-2023

Policy of Anti-Money Laundering Policy (AML)

This policy has been formed in the light of SEBI Circulars–on Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) as amended – obligations of Intermediaries under the Prevention of Money Laundering Act, 2002 ('Act') and Rules framed thereunder after making necessary amendments in the existing Anti-Money Laundering Policy of the Company. In pursuance of above said circular and the provisions of the Act, the policy of the company is to prohibit and actively prevent money laundering and any activity that facilitates money laundering or terrorist financing. Money Laundering (ML) is generally understood as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds or assets so that they appear to have been derived from legitimate origins or constitute legitimate assets.

1. Initiatives by Shivam infocom Private Limited - The basic purpose of the AML Policy is to establish a system for SIPL to participate in the international efforts against ML and to duly comply with the guidelines as detailed in the above circular of SEBI, as amended and other legal provisions and to ensure that SIPL is not used as a vehicle for ML. The AML framework of SIPL would meet the extant regulatory requirements.

2. Scope: This AML Policy establishes the standards of AML compliance and is applicable to all activities of SIPL.

3. Objectives of the Policy:

i. To establish a framework for adopting appropriate AML Procedures and controls in the operations / Business processes of SIPL.

ii. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

iii. To comply with applicable laws and regulatory guidelines.

iv. To take necessary steps to ensure that the concerned staff are adequately trained in KYC/AML procedures.

v. To assist law enforcement agencies in their effort to investigate and track money launderers.

4. Principal Officer – Designation and Duties:

The company has designated the Company Secretary as the Principal Officer for due compliance of its AML measures. He will 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. The duties of the Principal Officer will include monitoring the company's compliance with AML obligation and overseeing maintenance of AML records, communication and training for employees. The Principal Officer will ensure filing of necessary reports with the Financial Intelligence

Unit (FIU–IND). Principal Officer is authorized to issue additional circulars and advisories, to and seek information from the concerned officials for due compliance of AML measures from time to time.

The company has provided the FIU with contact information of the Principal Officer and will promptly notify FIU of any change in this information.

5. Customer Due Diligence:

At the time of opening an account the company will verify the identity records and current address(es) including permanent address(es) of the client, the nature of the business of the client and his financial status by scrupulously following the KYC norms. Adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship should be obtained. KYC norms shall be followed while establishing the client relationship and may further be followed while carrying out transactions for the client or when there is doubt regarding the veracity or adequacy of previously obtained client identification data.

Additionally following norms shall be observed:

i) No account will be opened in a fictitious, benami name or anonymous basis.

ii) Adhering to parameters developed to enable classification of clients into low, medium, and high risk.

iii) Documentation requirement and other information may be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of the Prevention of Money Laundering Act, 2002 and the guidelines issued by SEBI from time to time.

iv) The company shall consult the relevant authority, in case return of securities or money that may be from suspicious trades is desired.

v) Any person other than the constituent can operate the account of the constituent only if he/she has been duly authorized by the constituents. In case of body corporate or other entities, accounts can be operated only by the authorized persons supported by necessary documents. It is further clarified that the transaction limits for the operation, required margin and the trading relations with the clients will be governed as per the Circular, Rules, Regulations and Bye laws of SEBI/Exchange and as per agreement(s) with the constituents. It is further reiterated that all payments should be received by cheque and all payments should be made through cheque. Cash transactions are not allowed as per guideline and the company shall comply with the same.

vi) Before opening an account Company will 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 and may take declaration to this affect from the prospective client. On failure by prospective client to provide satisfactory evidence of identity, new account shall not be opened and the matter shall be reported to the higher authority.

vii) No accounts will be opened without acceptance of a copy of PAN Card. The said PAN received will be verified from the Income Tax/NSDL website before the account is opened.

viii) Without diluting the above requirements, the personnel opening a new account may obtain other independent information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

x) The Company shall duly comply with the KYC / client identification procedures that may be specified by SEBI from time to time.

xi) The concerned officials should take extra caution in case of existing or potential Politically Exposed Persons (PEP). They may seek additional information and also take the help of publicly available information.

xii) No business relationships can be established with PEP without the permission of any of the Directors of the Company or the Principal Officer. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, the approval from the above said officials is required to continue the business relationship.

xiii) The Officials of the Company may track the financial soundness of the clients and shall take reasonable measures to verify source of funds of clients identified as PEP.

7. Retention of Records:

The records of the identity of clients is maintained and preserved for a period of ten years from the date of cessation of transactions between the client and the Company. 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 retained until it is confirmed that case has been closed.

8. Monitoring Accounts for Suspicious Activity:

The following kinds of activities are to be treated as red flags and reported to the Principal Officer:

i. Clients whose identity verification seems difficult or clients appear not to cooperate ii.

ii. Where the source of the funds is not clear or not in keeping with client's apparent standing /business activity;

iii. Clients in high-risk jurisdictions or clients introduced by such clients or banks or affiliates based in high risk jurisdictions;

iv. Substantial increases in business without apparent cause;

v. Transfer of investment proceeds to apparently unrelated third parties;

vi. Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks financial services, businesses reported to be in the nature of export/import of small items.

The above-mentioned 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. When any functionary of the company detects any red flag, he or she will cause it to be further investigated for his/her satisfaction or report the same to the Principal Officer for further investigation and necessary action.

9. Reporting to Financial Intelligence Unit –India

In terms to the PMLA rules, Principal Officer is 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,
6th Floor, Hotel Samrat, Chankyapuri, New Delhi – 110021.
Website: http://fiuindia.gov.in

10. Internal Audit:

Internal Audit shall ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, 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.

11. Employee's Hiring /Employee's Training / Investor Education:

SIPL has an ongoing employee training under the leadership of the Principal Officer. The training includes, inter alia: 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 are the employees' roles in the company's compliance efforts and how to perform them; the company's record retention policy; and the disciplinary consequences for non-compliance with the Act. Means of the training may include educational pamphlets, videos, internet systems, in-person lectures, and explanatory memos. The operations are reviewed periodically to see if certain employees, such as those in compliance, margin, and corporate security, require additional specialized training. The implementation of AML/CFT measures requires intermediaries to demand certain information from investors which may be of personal nature or which have 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 customer with regard to the motive and purpose of collecting such information. Therefore, the Principal Officer and other officials of the company will sensitize the customers about these requirements as the ones emanating from AML and CFT framework so as to educate the customer of the objectives of the AML/CFT programme.

12 Monitoring Employee Conduct and Accounts:

SIPL subjects employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. The Principal Officer's account is reviewed by the Managing Director.

13 Confidential Reporting of AML Non-Compliance:

Employees report any violations of the company's AML compliance programme to the Principal Officer, unless the violations implicate the Principal Officer, in which case the employee shall report to the Managing Director. Such reports are confidential, and the employee suffers no victimization for making them.

14 Review

The Company conducts a periodic review of the policy. In case of amendment in statutory provisions/ regulations necessitating amendment, the relevant portions of policy shall be deemed to have been modified from the date of amendment in relevant statutory provisions. In such case the modified policy shall be placed for review by the Board in regular course.

15 Communication

Principal Officer shall ensure that this policy is communicated to all management and relevant staff including Directors, Head of the Department (s), customers and all concerned.

Prepared By
Piyush Mishra
Head HR

Approved By
Ashok Sharma
CFO

For Shivam Infocom Pvt. Ltd.

Authorised Signatory