GENERAL POLICY AND PROCEDURE

FOR

PREVENTION OF MONEY LAUNDERING

Based on Anti Money Laundering (AML) Standards/Combating Financing of Terrorism (CFT)/Obligations of Securities Market Intermediaries Under Prevention of Money Laundering Act, 2002 and Rules framed there-under

(As envisaged under the Prevention of Money Laundering Act, 2002)

Introduction to PMLA:

Objective: The objective of PMLA is to discourage and identify any money laundering and terrorist financing activities. The PMLA has come into force as result of international efforts to combat the terrorism and allied activities such as drug trafficking and other organized and serious crimes.

Nodal Agency: Financial Intelligence Unit – India (FIU-IND), set up by the Government of India as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister. The contact details of FIU-IND are as under:

Postal Address:
Director,
FIU-IND Financial Intelligence Unit – India,
6th Floor, Hotel Samrat Kautilya Marg,
Chanakyapuri,
New Delhi -110021, India.

Telephone: 91-11-26874473 (For Queries)
Fax: 91-11-26874459
Email: feedbk@fiuindia.gov.in (For Feedback)
query@fiuindia.gov.in (For General Queries)

1. Company Objective

The objective of this document is to effectively implement the provisions of Prevention of Money Laundering Act, 2002 (PMLA) and all the Rules and Regulations made there under, with a view to discharge its obligations under the said Act, Rules and Regulations and also to implement the guidance given by SEBI/NSE on the matter. This document may be amended from time to time in line with the future amendments under the said Act, Rules and Regulations.

2. Principal Officer Designation and Duties

The company has designated Mr. Mohamed H. Yacoobali (Chairman) as the Principal Officer for its Anti-Money Laundering Policy, with full responsibility for its implementation.

The duties of the Principal Officer will include monitoring the company's compliance with AML obligations and overseeing communication and training for employees namely; frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers. 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.

3. Policies and procedure of identifying/ acceptance of clients

- Entities such as individuals, HUFs, firms, public and private limited companies, non resident Indians and persons of Indian origin, etc., to be registered as a client after proper due diligence process in compliance with the guidelines and following know your client formalities prescribed by SEBI/exchanges.
- Further, no account will be opened in a fictitious / benami name or on an anonymous basis. It should be open by name, which disclosed in Income Tax PAN Card or Voter Identity card or Ration card or driving licenses.
- We should open beneficial account in the name of respective client only.
- We should analyze documents and information of suspicious client, which are given by client at the time of operating account.

Policy on Client Identification Programme

- We should take all the details and documentary evidence from our prospective client(s), which are required in our Member Constituent Agreement, risk disclosure document and KYC form, which should as per Exchange's circular no. NSE/INSP/2004/31 (Ref. no. NSE/INSP/5387) for KYC norms.
- We should take client details from reliable, independent source documents, data or information like Government Documentary evidence.
- We should check duplicate copy of original document with the original document.
- We should check 'Black List of Defaulter' on RBI site & SEBI site before making agreement with prospective client so that we can identify whether prospective client is defaulter or not.

- We should meet our prospective client 'Face to Face' for check the credit worth, capabilities and planning of client, which we cannot find out from information given by client for 'Client Registration Form'.
- We should allot a unique client code (UCC) to our clients, which should be Unique in nature and easy to identify the client.
- We should take details and information from client(s) as and when required.

4. Policy for risk categorization and clients of special category

Policy for Risk Categorization of clients :

All the clients registered with SGSSL shall be categorized into High Risk or Medium Risk or Low Risk from money laundering perspective. This categorization shall be done at the time of the registration of the client and be updated as and when required. Following are the factors of risk perception (in terms of monitoring suspicious transactions) of the clients :

- Client residential / office / correspondence address
- Background of the client
- Type of customer
- Nature of business activity carried out by the client
- Manner of making payments for the transactions undertaken
- Type of securities in which transaction entered
- Nature of transaction
- Trading Turnover
- Clients of special category as defined below

The high risk clients will require higher degree of due diligence in terms of monitoring suspicious transactions.

Clients of special category (CSC):

The following clients shall be classified as CSC:

a) Non-resident clients
b) High net worth clients,
c) Trust, Charities, NGOs and organizations receiving donations
d) Politically exposed persons (PEP) of foreign origin
e) Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
f) Companies offering foreign exchange offerings
g) 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.
h) Non face to face clients
i) Clients with dubious reputation as per public information available etc.

In addition to above, SGSSL shall exercise independent judgment to ascertain whether any client should be classified as CSC or not.

5. Maintenance of records

The Principal Officer will be responsible for the maintenance of following records:

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.
- 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 from any non monetary account such as demat account, security account maintained by the registered intermediary.

- Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith -
    - 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

- 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."

All the necessary records on transactions, records on customer identification shall be maintained as prescribed under the relevant act (PMLA, 2002 as well as SEBI ACT, 1992.)

6. Monitoring Accounts For Suspicious Activity

The specific nature of our business, organizational structure, type of our customers and transactions enable us to monitor manually / via front end terminals and Back Office Software for following example of alerts.

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

Broad categories of reasons for alerts are indicated as under:

- Identity of Client
  - False identification documents
  - Non face to face client

- Suspicious Background
  - Suspicious background or links with known criminals.

- Multiple Accounts
  - Unexplained transfers between multiple accounts with no rationale.
  - The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- Activity in Accounts
  - The customer engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, may warrant further due diligence to ensure the legitimacy of the customer's activity.
  - 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
  - Unusual or unjustified complexity
  - Investment proceeds transferred to a third party
  - Suspicious off market transactions

- Value of Transactions
  - Value just under the reporting threshold amount in an apparent attempt to avoid reporting
  - Large sums being transferred from overseas for making payments
  - Inconsistency in the payment pattern by client
  - Block deal which is not at market price or prices appear to be artificially inflated/deflated

- Procedures to be followed:
  - KYC procedures as prescribed by SEBI/Stock Exchange are to be followed while ascertaining the identity of the clients and opening the new accounts.
  - At the time of account opening the name of the client may be searched through the Internet search engines and the results, if any may be reviewed in the context of PMLA guidelines.
  - Identity Proof of Banking Account and Demat account shall be obtained before entering the details of bank and demat account in the client master database.
  - Back office software shall give alert in case of received cheques and demat deliveries is not matching with the master records.
  - Deliveries of demat shares shall be given only to the demat account Id registered in the master records. Payment of funds shall be given only by account payee cross cheques in favour of the account holder.
  - Third party payment of funds and delivery shall not be accepted or given.

- No cash shall be received from or paid to the clients towards the settlement obligation except as permitted by PMLA rules
- In case of payment being received by way of demand draft, pay order or any other mode where the identity of the account holder effecting the payment is not available, such payment instrument shall be accepted along with the covering letter from the person tendering the payment.
- The personnel in charge of day to day transactions in the key departments shall report to the Principal Officer, the details of those transactions which fall under the category or appears to be of the nature as mentioned above in this document.
- The recruitment of the new personnel at the key positions shall be confirmed after the verification of the document of identity, verification of address and reference from the known or reputed person.
- The assignment may be given to the outside agencies like Internal and/or Statutory Auditors or shall be created in house to review the appropriateness and adequacy of the internal control policy and procedures in the context of the size and nature of our business.

7. AML Record Keeping

Principal Officer will be responsible to ensure that AML records are maintained properly and preserved properly as per the relevant act, rules and regulations.

8. Reporting to FIU-IND

- For Cash Transaction Reporting
  We will not do any cash transaction hence reporting of cash transactions will not arise.
  However, in special circumstances, if we fall under cash dealing, we will follow the relevant act, rules and regulations.
- For Suspicious Transactions Reporting
  We will make a note of Suspicious Transactions that have not been explained to the satisfaction of the Principal Officer and thereafter principal officer will report the same to the FIU IND within the time limit as per relevant act, rules and regulations.
  Utmost confidentiality shall be maintained while filing reports to FIU-IND, and we shall ensure that there is no tipping off to the client at any level and account will be operated as per prevailing act, rules and regulations.

9. Training Programs

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

Training will include, at the minimum: how to identify alerts that arise during the course of the employees' duties; what to do once the risk is identified; what are employees' roles in the company's compliance efforts and how to perform them; the company's record retention and reporting policy, etc.

We will develop training in house, or contract for it. Attending regular seminars, referring the sites for any update on rules and regulation etc will be done.

Also the company will sensitize their customers about the objective of the AML/CFT programme.

We will review our operations to see if certain employees require specialized additional training.

10. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer.

11. 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 Officer, in which case employees shall report to the director of the company. Such reports will be confidential, and employees will suffer no retaliation for making them.

12. Approval of policy by the director of the company

We have approved this AML program as reasonably designed to achieve and monitor our company's ongoing compliance with the requirements of the PMLA and the implementing regulations under it.