PMLA POLICY

DSPL means Dhanki Securities Private Limited. The policy was first made at the time of applicability of the PMLA requirements and has been later reviewed at various occasion with the latest reviewing being done on 20th September, 2021 covering the various circular issued by FIU/SEBI.

The below mentioned policy on PMLA has been approved by the Board of Directors in their meeting and has been adopted by the company (broking house). All the employees are required to follow the same and take due care for its proper implementation and efforts are to be made to make this known to the clients who deal with the company.

Procedures with respect to implementation of Anti Money Laundering Measures under the Prevention of Money Laundering Act, 2002.

1. Objective:
   The objective of these measures is to discourage and identify any money laundering or terrorist financing activities. These measures are intended to place a system for identifying; monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

2. Appointment of Principal Officer:
   The company shall appoint a Principal Officer, as required under the Prevention of Money Laundering Act, 2002. The Principal Officer is responsible to discharge the legal obligations to report suspicious transactions to the authorities. The Principal Officer will act as a central reference point in facilitating onward reporting of suspicious transactions and assessment of potentially suspicious transactions. In case of any change in the Principal Officer, the information regarding the same would be immediately informed to FIU.

3. Appoint a Designated Director:
   As defined in Rule 2 (ba) of the PML Rules, the company shall appoint a Designated Director who should be responsible for ensuring the compliance with the PMLA requirements;
   "Designated Director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes the Managing Director or a Whole-time Director duly authorized by the Board of Directors.

4. Information's to be recorded:
   - 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.
   - The parties to the transaction.

5. Transactions to Record:

- 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 and where any forgery of a valuable security has taken place.
- All suspicious transactions whether or not made in cash are reviewed.

Note: For recording all the suspicious transactions "transactions integrally connected", "transactions remotely connected or related" should also be considered in records.

6. Records Maintenance:

- The Company shall maintain adequate records so as to enable it to demonstrate that appropriate initial and ongoing Customer Due Diligence procedures have been followed. To this end, Company shall maintain records of
  (i) Client Identification Procedure
  (ii) All documents collected at the time of client on-boarding
  (iii) Customer Risk Profiling

- Adequate records of all transactions should be maintained in order to permit reconstruction of transactions including the amounts, types of currency involved, the origin of funds received into customer's accounts and the beneficiaries of payments out of customer's accounts. To this end, the Company shall retain following information for the account of their customers in order to maintain a satisfactory audit trail:
  a. the beneficial owner of the account;
  b. the volume of the funds flowing through the account; and
  c. for selected transactions:
     - the origin of the funds;
     - the form in which the funds were offered or withdrawn, e.g. cheques, EFT, etc.;
     - the identity of the person undertaking the transaction;
     - the destination of the funds;
     - the form of instruction and authority.

- As per Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018" & SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18th, 2020 all necessary records on transactions, both domestic and international, should be maintained at least for the minimum period of 10 years as prescribed in PMLA, 2002 or in any other legislations, regulations, exchange byelaws or circulars.

- In situation 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.
- The company should record and maintain and preserve the information regarding the transaction as provided in Rule 3 of the PML rules and the information of the same should be maintained for a period of 10 years or until the closure of the trail for the trade.
- DSPL shall register the details of a client, in case of client being a non-profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

7. Procedure and manner of maintaining information:

- The company shall maintain information in respect of above transactions with its client in hard and soft copies and in accordance with the procedure, as the case may be, from time to time.

8. Monitoring & Reporting of Transactions:

- The company has a system of monitoring the transactions by the principal officer which are reviewed. The principal officer also reviews the alerts provided by the exchanges, SEBI and the same is reviewed so as to enquire the genuinity of the transaction. Additionally, the transactions done are checked manually so as to determine the authenticity of the trade.
- The company carries out due diligence and scrutiny of transactions to ensure that the transactions being conducted are consistent with the business and risk profile of the client on the basis of the information provided by the clients.
- The principal officer would further investigate the transactions and call for further information as required. If felt suspicious the principal officer would inform immediately to the Financial Intelligence Unit (FIU) giving details of the transaction in the Suspicious Transaction Report (STR).
- The proper documents and supporting for the transaction should be maintained with the intermediary and forward the details as may be called by the regulators.

In terms of the PML Rules, intermediaries 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,
6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi-110021.
Website: http://fiuindia.gov.in

and shall adhere to the following instructions given in SEBI Master Circular no. SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113 dated October 15, 2019 while reporting

- The CTRs (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month;

b. Suspicious Transaction Reports (STRs):
   - All suspicious transactions shall be reported by the Principal Officer to Director, FIU-IND within 7 working days of establishment of suspicion at the level of Principal Officer. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

c. The Principal Officer will be responsible for timely submission of CTRs and STRs to FIU-IND;

d. Utmost confidentiality should be maintained in filing of CTRs and STRs to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.

e. No NIL reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

Every control system should be established in the organization to take care that the reporting of suspicious activity should be done to the regulators only and no client should be informed to the suspicious reporting being done about themselves or about anybody else. The Company and its staff are strictly required to ensure that there is no 'tipping-off' to any customers about any suspicious transaction reporting that has been made to the regulators. The organization may use the learning from the suspicious activity to train the staff for controlling any suspicious activity and use the information for investor / clients awareness about the suspicious transactions

9. Policy and procedures to Combat Money Laundering and Terrorist Financing

Company has resolved that it would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a frame work for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to FIU as per the guidelines of PMLA Rules, 2002. Further, member shall regularly review the policies and procedures on PMLA and Terrorist Financing to ensure their effectiveness.

To be in compliance with these obligations, the senior management of DSPL shall be fully committed to establishing appropriate policies and procedures for the prevention of Money Laundering and Terrorist Financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The Registered Intermediaries shall:

(a) Issue a statement of policies and procedures, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;

(b) Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, DSPL shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

(c) Ensure that the content of these Directives are understood by all staff members;

(d) Regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;

(e) Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;

(f) Undertake client due diligence ("CDD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

(g) If DSPL is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the DSPL shall not pursue the CDD process, and shall instead file a STR with FIUIND.

(h) Have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and

(i) Develop staff members' awareness and vigilance to guard against ML and TF

10. Customer Due diligence:

a. Identification / Verification of clients:

The company has system in place for acceptance of new client. The main measures which company has implemented for acceptance of new client keeping in view the PMLA requirements are as follows:

1. The Application forms for opening an account are issued to prospective client if he provides a valid reference.
2. All accounts are opened only when the prospective client is present in person before the company official.
3. The company collects the details of location (permanent address, correspondence address and registered office address), occupation details, nature of business activities, financial details etc. before new clients is registered.
4. The company shall collect the various mandatory documents as required by law, including the proof of identity of the client. The company should check the reliability of the document by reviewing / checking the same from independent source like verifying the PAN from the income tax website, etc.
5. The company has a procedure to determine whether existing / potential client are not Politically Exposed Person (PEP) and in case of any person found to be a PEP entity then approval of senior management is necessary.
6. Check that the identity of the clients 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.

7. The company has a system in place to ensure that accounts are not opened in the name of anyone whose name appears in the UN or SEBI debarred entities and the scan of all existing accounts are carried out.
8. The company periodically reviews the trading volumes of the clients and their financial strength in terms of annual income, net worth etc.
9. The company also monitors the financial transactions with clients for pay in payout of funds and securities.
10. The company has the policy not to deal in cash with any of the clients, all transactions, receipt or payment, are carried out only through account payee cheque or Electronic Fund Transfer only.
11. All funds are released to the client by account payee cheques issued in clients name only or by RTGS or by NEFT to clients bank account.

b. Policy for acceptance of Customers

Company has developed customer acceptance policies and procedures which aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. The following safeguards are followed while accepting the customers.

i. No Trading account is opened in a fictitious / benami name, Suspended / Banned Organization and person.
ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to Customers' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc and manner of making payment for transactions undertaken. These parameters enable classification of Customers into low, medium and high risk. Customers of special category (as given below) are classified under higher risk. Higher degree of due diligence and regular update of Know Your Clients profile are carried for these Customers.

Clients of special category (CSC) include the following:

- Non-resident clients
- High net-worth clients,
- Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations,
- Companies having close family shareholdings or beneficial ownership
- Politically Exposed Persons (PEP)
- Companies offering foreign exchange offerings
- 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 repute any of the following – Havens / sponsors of