MARKET PULSE SECURITIES PVT. LTD.

ANTI MONEY LAUNDERING POLICY

Version	1.0
Prepared by	Compliance team of MPSPL
Approved by	Board of Directors of MPSPL

TABLE OF CONTENTS

ANTI MONEY LAUNDERING POLICY

1. OBJECTIVE OF THIS POLICY

The objective of this Anti Money Laundering Policy ('Policy) is to guide all the employees of Market Pulse Securities Pvt. Ltd. ('MPSPL'/ 'Company'**)** and employees of its associates on the steps that they are required to take and implement to prevent and identify any Money Laundering (ML) or Terrorist Financing (TF) activities and obligations to be followed to ensure compliance with issues related to Know Your Client (KYC) Norms, Anti Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing Of Terrorism (CFT).

It shall be the responsibility of each of the concerned employees that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the "Prevention of Money Laundering Act, 2002". This policy specifies the need for additional disclosures to be made by the clients to address concerns of Money Laundering and Suspicious transactions (STR) undertaken by clients and reporting to FIU.

2. BACKGROUND

The Government of India has serious concerns over money laundering activities, which are not only illegal but anti-national as well. Money laundering is the process by which large amount of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from a legitimate source. All crimes that produce a financial benefit give rise to money laundering.

Pursuant to the recommendations made by the Financial Action Task Force (FATF), SEBI vide its Circular No. ISD/CIR/RR/AML/1/06 dated January 18 2006, Circular No. ISD/CIR/RR/AML/2/06 dated March 20, 2006 and Circular No. CIR/MIRSD/1/2014 dated March 12, 2014 had issued the guidelines on Anti Money Laundering Standards. As per these SEBI guidelines, all registered intermediaries have been advised to ensure that proper policy frameworks are put in place and they shall be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

As a market participant it is evident that strict and vigilant tracking of all transactions of suspicious nature is required.

3. FINANCIAL INTELLIGENCE UNIT

The government of India set up Financial Intelligence Unit -India (FIU) on 18th November 2004 as an independent body to report directly to the Economic Intelligence council (EIC) headed by the Finance Minister. FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transaction. FIU-IND is also responsible for coordinating and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against Money laundering and related Crimes.

4. THE PREVENTION OF MONEY LAUNDERING ACT, 2002

The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1st July, 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

As per the provisions of the PMLA, every banking company, financial institution and intermediary shall have to adhere to client account opening procedures and maintain records of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include;

All cash transactions of the value of more than Rs 10 lacs or its equivalent in foreign currency.

All series of cash transactions integrally connected to each other which have been valued below Rs 10 lacs or its equivalent in foreign currency where such series of transactions take place within one calendar month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency

All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits from any non monetary account such as Demat account, security account maintained by the registered intermediary.

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.

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

1. gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
2. appears to be made in circumstances of unusual or unjustified complexity or
3. appears to have no economic rationale or bonafide purpose.
4. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism
5. Identity verification or address details seems difficult or found to be forged / false
6. Asset management services where the source of the funds is not clear or not in keeping with apparent standing /business activity
7. Substantial increases in business without apparent cause
8. Unusual & Unexplained large value of transaction
9. Transfer of large sums of money to or from overseas locations
10. Unusual & Unexplained activity in dormant accounts

This Policy only supplements the existing SEBI / FIU guidelines relating to KYC/AML and any subsequent guidelines from the date of the Policy on KYC/AML will be implemented

immediately, with subsequent ratification by the Board. Extant regulations will at any point in time override this Policy.

5. WHAT IS MONEY LAUNDERING

Money Laundering (ML) is the process of disguising the illegal origin of criminal proceeds. It is a process by which persons with criminal intent or persons involved in criminal activities attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of illegal funds.

In simple terms money laundering is most often described as the “turning of dirty or black money into clean or white money”. If undertaken successfully, money laundering allows criminals to legitimize "dirty" money by mingling it with "clean" money, ultimately providing a legitimate cover for the source of their income.

Although money laundering is a complex process, it generally follows three stages:

Placement is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is structuring— breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or recordkeeping requirements.

Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.

Integration is the final stage in the re-injection of the laundered proceeds back into the economy in such a way that they re-enter the financial system as normal business funds. Banks and financial intermediaries are vulnerable from the Money Laundering point of view since criminal proceeds can enter banks in the form of large cash deposits.

Three most common stages of Money Laundering, as mentioned above are resorted to, by the launderers. The laundered proceeds re-enter the financial system appearing to be normal business funds and Market Intermediaries may unwittingly get exposed to a potential criminal activity while undertaking such normal business transactions.

6. WHY “KNOW YOUR CUSTOMER”

One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer’s business and pattern of financial transactions. The adoption of procedures by which financial institutions “know their customer” is not only a principle of good business but is also an essential tool to avoid involvement in money laundering.

MPSPL shall adopt appropriate KYC procedures and internal controls measures to:

a. Determine and document the true identity of the customers who establish relationships, open accounts or conduct significant business transactions and obtain basic background information on customers;
b. Assess the money laundering risk posed by customers' expected use of MPSPL's products and services;
c. Protect MPSPL from the risks of doing business with any individual or entity whose identity cannot be determined or who refuses to provide information, or who have provided information that contains significant inconsistencies which cannot be resolved after due investigation.

7. CLIENT DUE DILIGENCE

The main aspect of this policy is the Customer Due Diligence Process which means:

a. To obtain sufficient information in order to identify persons who beneficially own or control the securities account. 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 shall be identified using client identification and verification procedures.
b. To verify the customer's identity using reliable, independent source document, data or information.
c. To identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted;
d. To 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 consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and
e. To periodically update all documents, data or information of all clients collected under the CDD process.
f. All new clients shall be reviewed against the negative list issued by the SEBI, Exchanges and other lists such as UN sanction lists.
g. In person verification to be carried out in terms of the regulatory requirements prescribed by regulators.

The Customer Due Diligence process includes three specific parameters:
- Client Acceptance Policy
- Client Identification Procedure
- Suspicious Transaction identification and reporting

8. CLIENT ACCEPTANCE POLICY

Our client acceptance policies and procedures aims to identify the types of clients that are likely to pose a higher than average risk of ML or TF so that we will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transactions.

The following safeguards shall be followed by the MPSPL while accepting the clients:

a. Accept clients on whom we are able to apply appropriate KYC Procedures - Obtain complete information from the client. It should be ensured that the initial forms taken by the client are filled and checked completely without any exception. Ensure that the 'Know Your Client' guidelines are followed without any exception. All supporting documents as specified by Exchange and SEBI are obtained and verified.
b. No client account shall be opened in a fictitious / benami name or on an anonymous basis.
c. Factors of risk perception (in terms of monitoring suspicious transactions) of the client shall be defined having regard to -
    - Clients' 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.

    The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require a higher degree of due diligence and regular update of Know Your Client (**KYC**) profile.

d. Documentation requirements and other information shall be collected in respect of different classes of clients depending on the 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.
e. MPSPL shall not open an account or close an existing account where the Company is unable to apply appropriate CDD measures/ KYC policies. It shall apply 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.
f. If at the time of establishing the intermediary – client relationship, it is suspected that the prospective client has a suspicious background or links with known criminals or is banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide; the account will not be activated.
g. The prospective client's name shall also be compared with the list of people who are barred from dealing / trading as mentioned on the Exchanges/ SEBI websites. If it is established that the prospective client is so barred then his /her account shall not be activated. Moreover, a Self Declaration, stating that they have not been involved in any criminal offense and neither has been barred from dealing / trading by Exchange/SEBI shall be taken from all clients.
h. Clients Of Special Category - MPSPL shall take utmost care while dealing with a client of Special Category. Such clients shall include:
    - Non-Resident clients,
    - Trust, Charities, NGOs, Organization receiving donation,
    - Companies having closed shareholding/ownership,
    - PEP - Politically Exposed Persons (PEP) 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. The additional norms applicable to PEP shall also be applied to the accounts of the family members or close relatives of PEPs.

- Persons of foreign origin, companies dealing in foreign currency, shell companies, overseas entities, Companies offering foreign exchange, etc.
- Non face to face clients
- Clients with dubious background
- Clients from 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 Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. While dealing with clients in high risk countries other than FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), we shall also independently access and consider other publicly available information.
- High Net worth clients: High net worth clients could be classified if at the account opening stage or during the course of the relationship, it is realized that the client's investments or the appetite for investment is high. The High net worth clients are basically categorized as the clients having a Net worth of Rs. 10 Crores or more.

MPSPL shall scrutinize minutely the records/documents pertaining to clients belonging to the aforesaid category. The client of a special category should be categorized as a high-risk client. MPSPL shall closely examine the transaction in order to ensure they are consistent with Client business and risk profile. In the case of the High-risk category due care and caution shall be exercised at the acceptance stage itself. The profile of such Clients has to be updated regularly.

i. No account can be opened in the name of an individual or entity whose name is listed on the banned entity list being maintained at United Nation's website at & also as published on Exchanges & SEBI website.
j. No account can be opened by the persons covered under the list of high risk countries as provided by FATF.
k. Documents received from clients during the client due diligence (CDD) process should be reviewed & updated on an annual basis or as per information provided by clients.

9. RISK – BASED APPROACH

Client acceptance is a critical activity in AML compliance. Registering any client means providing such client with an entry point to local and international financial systems. Client acceptance, thus, becomes the first step in controlling money laundering and terrorist financing.

Regulatory guidelines stipulate that a sound KYC program should determine the true identity and existence of the customer and the risk associated with the customer. It is therefore imperative that we capture information about their background, sources of funds, nature and type of business, domicile and financial products used by them and how these are delivered to them in order to properly understand their risk profile.

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. The basic principle enshrined in this approach is an enhanced client due diligence process shall be required to be adopted for higher risk categories of clients and 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 we shall obtain necessarily depend on the risk category of a particular client and for this purpose clients may be classified into following categories namely;-

(i) High Risk

Clients defined in a special category, clients who have defaulted in the past, have suspicious background, and do not have any financial status are classified as high risk.

All transactions of Clients identified as High Risk Category should be put to counter measures. These measures may include further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of transactions and applying enhanced due diligence.

(ii) Medium Risk

Clients that are likely to pose a higher than average risk to the broker may be categorized as medium risk depending on Client's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

- Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
- Where the client profile of the person/s opening the account, according to the perception of the team is uncertain and/or doubtful/dubious.

Further, Clients who are mostly intra-day Clients or speculative Clients or Clients maintaining a running account continuously with the Company may also be categorized as Medium risk clients on a case to case basis.

(iii) Low Risk

Clients pose Nil or low risk. Individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc.

They are Individuals/Corporate/HNIs who have respectable social and financial standing. These are the Clients who make a payment on time and take delivery of shares.

The low risk provisions should not apply when there are suspicions of Money Laundering / Terrorism Financing (ML/TF) or when other factors give rise to a belief that the customer does not in fact pose a low risk.
Any change in the risk profile of the client, has to be ascertained on a regular basis. An assessment should be made of the financial worthiness of the client by obtaining appropriate declarations at KYC stage. This information should be subsequently used for monitoring whether the transactions of the clients are within the declared means and if the value of the transactions is increasing the client should be asked to disclose the increasing sources

10. RISK ASSESSMENT

a. MPSPL will be carrying out risk assessment to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. 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 namely UNSC_1267, UNSC_1988, UNSC_2140 and UNSC_2270 (these can be accessed at https://www.un.org)
b. The risk assessment carried out shall also 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 by them.

11. CLIENT IDENTIFICATION PROCEDURE

Client identification means verifying the identity of clients/potential clients by using reliable and independent source data or documents. The procedure shall include -

a. Obtain sufficient documentation and information at the time of opening an account, adequate enough to satisfy competent authorities (regulatory / enforcement authorities) for the identification of clients. Further, the additional documents or information shall be collected from different classes of clients on the basis of the perceived risk and after having regard to the requirements of the Prevention of Money Laundering Act 2002 and the guidelines issued by Exchange and SEBI from time to time.
b. Identification procedure is to be carried out at the following 3 stages:
   While establishing the intermediary – client relationship;
   While carrying out transactions for the client;
   When there are doubts regarding the veracity or the adequacy of previously obtained client identification data.
c. Appropriate risk management systems put in place to determine whether the client or potential 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.

d. Senior management approval shall be obtained 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, senior management approval to be obtained to continue the business relationship.
e. Reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
f. Conduct of an ongoing due diligence and scrutiny of the transactions and client's account, throughout the course of the business relationship shall be done to ensure that the transactions being conducted are consistent with the client's business and risk profile, taking into account, where necessary, the customer's source of funds.

The underlying objective of client identification procedure is to follow the requirements preserved in the PMLA, SEBI Regulations, directives and circulars issued and so as to be aware of the clients on whose behalf the company is dealing.

12. RELIANCE ON THIRD PARTY FOR CARRYING OUT CLIENT DUE DILIGENCE

MPSPL 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 parties 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.

Such reliance shall be subject to conditions that are specified in rule 9(2) of the PML Rules and further in line with the regulations and circular / guidelines as may be issued by SEBI from time to time.

13. MONITORING OF TRANSACTIONS

MPSPL shall have in place a comprehensive transaction monitoring process from a KYC/AML perspective. MPSPL shall put in place strong transaction alerts which will provide proactive signals on suspicious transactions and possible money laundering and the list shall be updated based on current understanding of the market scenario and trading patterns followed by clients. Regular monitoring of transactions is required for ensuring effectiveness of the Anti Money Laundering procedures.

MPSPL will pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose.

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 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.

Record of the transactions in terms of Section 12 of the PMLA shall be preserved and those transactions of a suspicious nature or any other transactions notified under Section 12 of the Act shall be reported to the Director, FIU-IND. Suspicious transactions shall be regularly reported to the Senior Management.

14. SUSPICIOUS TRANSACTION MONITORING AND REPORTING

What is a Suspicious Transaction?

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 circumstance of unusual or unjustified complexity; or
Appears to have no economic rationale or bona fide purpose

Reasons for Suspicious:

Identity of client

- False identification documents
- Identification documents which could not be verified within reasonable time or clients appear not to cooperate
- Non-face to face client
- Clients in high-risk jurisdiction
- Unusual transactions by Clients of Special Categories (CSCs)
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities
- Suspicious background or links with criminals

Multiple Accounts

- Large number of accounts having a common parameters such as common partners / directors / promoters / address/ email address / contact numbers introducer or authorized signatory
- Unexplained transfers between such multiple accounts.

Activity In Accounts

- Unusual activity compared to past transactions
- Use of different accounts by client alternatively
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business
- Account used for circular trading

Nature Of Transactions

- Unusual or unjustified complexity
- No economic rationale or bonafied purpose

- Source of funds are doubtful
- Appears to be case of insider trading
- Purchases made on own account transferred to a third party through an off market transactions through DP account
- Transactions reflect likely market manipulations
- Suspicious off market transactions

Value Of Transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Inconsistent with the clients apparent financial standing
- Inconsistency in the payment pattern by client
- Block deal which is not at market price or prices appear to be artificially inflated/deflated

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, MPSPL will file STR if there are reasonable grounds to believe that the transactions involve proceeds of crime.

Reporting of Suspicious Transaction

- Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer, Compliance Officer, Principal Officer or any other designated officer.
- 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.
- The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record the reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such a report shall be made available to the competent authorities on request.
- While ensuring that there is no tipping off to the customer at any level, MPSPL may put restrictions on operations in the accounts where an STR has been made.

15. RECORD KEEPING REQUIREMENTS & RETENTION OF RECORDS

MPSPL shall preserve records pertaining to transactions of clients for a period of five years from the date of the transaction. Record of documents evidencing the identity of the clients (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence shall be maintained and preserved for a period of five years even after the business relationship with the client has ended or the account has been closed, whichever is later. Records shall be maintained 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 behavior or if there be any suspected drug related or other 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, the following information of the client shall be maintained by MPSPL 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:
    i. the origin of the funds
    ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts, etc.
    iii. the identity of the person undertaking the transaction;
    iv. the destination of the funds;
    v. the form of instruction and authority.

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, shall be maintained and preserved for a period of five years from the date of the transaction with the client.

In the case of transactions where any investigations by any authority has been commenced and in the case of transactions which have been the subject of suspicious transactions reporting all the records shall be maintained till the authority informs of closure of the case.

Following information in respect of transactions referred to in Rule 3 of PML Rules shall be maintained by MPSPL:

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

16. LIST OF DESIGNATED INDIVIDUALS OR ENTITIES

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at http://www.un.org/sc/committees/1267/consolist.shtml.

Precaution shall be taken to ensure that no account is opened whose name shall be appearing in such a list.

Periodic review of the existing account shall be conducted to ensure that no existing account is linked to any of the entities or individuals included in the list.
Any resemblance found shall be reported to SEBI and FIU-IND.

17. REPORTING TO FIU

In terms of the PMLA rules, brokers and sub-brokers are required to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) as per the schedule given below:

Report	Description	Due Date
STR	All suspicious transactions whether or not being made in cash	Not later than seven days on satisfied that the transaction is suspicious

The Principal Officer will be responsible for timely submission of STR to FIU-IND. Utmost confidentiality shall be maintained in filing of, STR to FIU-IND. No nil reporting needs to be made to FIU-IND in case there are no suspicious/ non – profit organization transactions to be reported.

18. PROCEDURE FOR FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES

For implementation of section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), i.e. freezing and unfreezing of funds, financial assets of economic resources, MPSPL shall follow the procedure as laid down in Order issued by Central Government.

19. PRINCIPAL OFFICER

The Company has designated Ms. Hiral Jain, Co-founder, Director and Chief Financial Officer of the Company, as the Principal Officer in terms of the requirement of the PMLA Act. The Principal Officer shall be responsible for implementation and compliance of this policy shall include the following:

- Compliance of the provisions of the PMLA and AML Guidelines
- Monitoring the implementation of Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) Policy
- Reporting of Transactions and sharing of information as required under the law
- Ensuring submission of periodical reports to Senior Management. The report shall mention if any suspicious transactions are being looked into by the respective business groups and if any reporting is to be made to the authorities.
- Ensure that MPSPL discharges its legal obligation to report suspicious transactions to the concerned authorities.

20. DESIGNATED DIRECTOR

The Company has appointed Mr. Arshad Fahoum, Director & Chief Product Officer of the Company, as the “Designated Director” for ensuring overall supervision and compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules.

21. SYSTEM AND PROCEDURE FOR HIRING OF EMPLOYEES

We do adequate screening procedures while hiring employees and also ensure that the employees dealing with PMLA requirements are suitable and competent to perform their duties. The Company shall take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting.

22. EMPLOYEES TRAINING

- Importance of PMLA Act & its requirement shall be communicated to employees through training.
- Ensuring that all the operating and management staff fully understands their responsibilities under PMLA for strict adherence to customer due diligence requirements from establishment of new accounts to transaction monitoring and reporting suspicious transactions to the FIU.
- Organizing suitable training programmes wherever required for new staff, front- line staff, supervisory staff, etc.
- Adequate training should be given to all the concerned employees to (a) ensure that the contents of the guidelines are understood and (b) develop awareness and vigilance to guard against money laundering and terrorist financing.

As of now, AML policy will be covered during the induction training given to all new recruits and also during the on-going compliance sessions.

Records of all staff who have undertaken AML training are maintained by the Compliance Team.

23. INVESTOR'S EDUCATION

As the implementation of AML/CFT measures being sensitive subject and requires us to demand and collect certain information from investors which may be of personal in nature or has hitherto never been called for, which information include documents evidencing source of funds/income tax returns/bank records etc. and can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. MPSPL shall prepare this specific literature so that the clients can be educated on the objectives of the AntiMoney Laundering (AML) / Combating Financing of Terrorism (CFT) programme. The importance of the same is also made known to them at the time of opening the Account.

24. REVIEW OF POLICY

The Policy shall be reviewed from time to time as and when required by the Management or to implement the changes as laid down in Anti Money Laundering Act, 2002 or change in any other applicable Act, Rules, Regulations, Bye-Laws.