

**KNOW YOUR CUSTOMER
&
ANTI MONEY LAUNDERING POLICY**

**ADOPTED BY
ASNANI STOCK BROKER PRIVATE LIMITED**
MEMBER BSE, NSE, MCX NCDEX, CDSL

Table of Contents

Preface

1. ASBPL Initiatives & Philosophy
2. What is Money Laundering?
3. Principal Officer - Designation and Duties
4. Designated Director - Designation and Duties
5. Know your customer
6. Customer Acceptance policy
7. Customer Due Diligence
8. Customer Identification Procedure
9. Monitoring of Transactions
10. Risk Management
11. Combating Financing of Terrorism
12. Maintenance of Records
13. Retention of Records
14. Reporting to Financial Intelligence Unit - India
15. Employees Hiring /Employees Training / Investor Education

Preface

This is the Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy (the Policy) of ASNANI STOCK BROKER PRIVATE LIMITED (ASBPL) and has been prepared in accordance Prevention of Money Laundering Act, 2002 (PMLA Act). This Policy also takes into account the provisions of the PMLA Act and other Rules laid down by SEBI/FMC/CDSL/EXCHANGES, and FIU. The earlier policy framed on 21.05.2013, has been reviewed in the light of SEBI Circular No. CIR/MIRSD/1/2014, March 12, 2014 on Guidelines on Identification of Beneficial Ownership, 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 Prevention of Money Laundering Act, 2002 (PMLA) and CDSL Communiqué 542 dated 25-Oct-2019 for review of policy, the policy of the company is to prohibit and actively prevent money laundering and any activity that facilitates money laundering (ML) or terrorist financing. Money laundering 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 derived from legitimate origins or constitute legitimate assets.

As per PMLA, every banking company, financial institution (which includes chit fund company, a cooperative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities/commodities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA. For the purpose of PMLA, transactions include:

1. All cash transactions of the value of more than Rs 10 Lakh or its equivalent in foreign currency.
2. All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakh or its equivalent in foreign currency, such series of transactions within one calendar month.
3. 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.

For the purpose of suspicious transactions reporting, apart from „transactions integrally connected, „transactions remotely connected or related need to 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.

1. ASBPL Initiatives & Philosophy

ASBPL had undertaken a comprehensive review of its AML framework and laid down an Anti Money Laundering Policy in 2006 which was reviewed from time to time.

The basic purpose of this AML Policy is to establish a system for “Client Due Diligence Process” for ASBPL to participate in the international efforts against ML and to duly comply with the detailed guidelines as described under above said circular of SEBI/FMC and other legal provisions as well as to ensure that ASBPL is not used as a vehicle for ML. The AML framework of the ASBPL would meet the extant regulatory requirements.

It is important that ASBPL management views “money-laundering prevention” and “knowing your customer” as part of the risk management strategies and not simply as standalone requirements that are being imposed by legislation/regulators”.

Hence the objective of the policy is to -

1. To have a proper Customer Due Diligence (CDD) process before registering clients.
2. To monitor/maintain records of all cash transactions of the value of more than Rs.10 lacs.
3. To maintain records of all series of integrally connected cash transactions within one calendar month.
4. To monitor and report suspicious transactions.
5. To discourage and identify money laundering or terrorist financing activities. To take adequate and appropriate measures to follow the spirit of the PMLA

2. What is Money Laundering?

Money laundering is the criminal practice of putting dirty money through a series of transactions, so that the funds are cleaned to look like proceeds from legal activities. It is driven by criminal activities and conceals the true source, ownership, or use of 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.

Section 3 of the PMLA Act defines money laundering in following words:

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering”.

3. Principal Officer – Designation and Duties

The company has designated Mr. Vinod Asnani, as the Principal Officer for due compliance of its Anti-Money Laundering Policies. 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 compliance with AML obligations 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 policies 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.

4. Designated Director – Designation and Duties

The company has designated Mr. Vinod Asnani, as the Designated Director to ensure overall compliance with the obligations imposed under chapter IV of the Act and Rules.

5. 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.

ASBPL 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 ASBPL products and services;
- c) Protect ASBPL 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.

6. Customer Acceptance Policy

No account shall be opened in anonymous or fictitious / benami name(s). PAN shall be mandatory for each account. Each client shall have one account only.

The parameters of risk perception in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc shall be captured at the account opening stage to enable categorization of customers into

low, medium and high risk.

For the purpose of risk categorization, individuals/entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. Illustrative examples of low risk customers are as follows:

- Salaried employees whose salary structures are well defined;
- Government Departments and Government owned companies;
- regulators and statutory bodies; etc.

Customers that are likely to pose a higher than average risk to ASBPL shall be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. ASBPL shall apply Customer Due Diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

7. Customer Due Diligence

The Company will exercise Customer Due Diligence (CDD) in client acceptance and subsequent continuing relationship with the clients. It will include:

- (a) Obtaining sufficient information in order to identify persons who beneficially own or control the securities/commodities account. Whenever it is apparent that the securities/commodities 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. The beneficial owner is the natural person or persons, who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
- (b) Verify the clients identity using reliable, independent source documents, data or information;
- (c) 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) Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);
- (e) Understand the ownership and control structure of the client;
- (f) 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 Company knowledge of the client, its business and risk profile, taking into account, where necessary, the

clients source of funds; and

- (g) Annually updating all documents, data or information of all clients and beneficial owners collected under the CDD process.

While implementing CDD procedures the Company, in accepting a new client, shall:

- i. Adopt a Risk Based Approach
 - ii. Verify proofs of identity, address, and financial status of the client and persons acting on its behalf, ownership and control structure by scrupulously following the KYC norms of the relevant exchange/RBI. 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 the adequacy of previously obtained client identification data. Account should be opened only after the completion of all the required documents and after due verification with originals. In person verification shall be carried in a manner provided by SEBI/FMC/Exchange. Where permitted by SEBI/FMC/Exchange the Company may rely on the information/CDD by KRA.
 - iii. Not open any account in a fictitious / benami name or on an anonymous basis .ensure that the identity of the proposed client does not match with any person having known criminal background and his is not banned in any other manner, whether in terms of UN sanction resolutions available on website at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml> or orders of any other enforcement agency.
-

While accepting and executing a client relationship the Company will adopt a Risk Based Approach as under:

| Low Risk | Medium Risk | High Risk |
|--|--|---|
| Individual clients, with clean image, not PEP, with investment upto Rs. 10 Lakhs, whose identity and sources of wealth can be easily identified. | Clients over investment of Rs. 10 Lakhs where identity and sources of wealth are not supported by public documents like Income Returns, Registered conveyance Deeds etc. | HNI Clients with no known sources of Income |
| Listed Companies | Clients with sudden spurt in volumes or investment without apparent reasons | Clients subsequently becoming suspicious of ML/FT activities |
| Govt. owned companies, regulated bodies like banks and PMLA regulated intermediaries Day traders and arbitrageurs | Persons in business/industry or trading activity where scope or history of unlawful trading/business activity dealings is more. Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious . | Single Share Companies Or Companies with bearer Shares |
| Clients having regular relationship or low volumes (e.g. upto 10 lakhs) | Clients having occasional relationship but with moderate volumes (10 - 50 lakhs) | Clients having occasional relationship with large volumes (over 50 lakhs) |
| | | Politically Exposed Persons Systems should be there to find out whether a person is PEP- Take reasonable measures to establish source of wealth and source of funds on ongoing basis. Client accounts opened by professional intermediaries |

In case of Low Risk Clients only the basic requirements of verifying the identity and location of the customer may be sufficient. Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk. In case of Medium Risk Clients, some public or market information should also be gathered and sources of funds for transactions should be tracked on ongoing basis. The decision to open a High Risk Client account should be taken only by the Senior Management.

The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

Clients of Special Category: Special care shall be taken while opening accounts of Clients of Special Category. Such clients include the following

- a. Non resident clients
- b. High Networth clients,
- c. Trust, Charities, NGOs and organizations receiving donations
- d. Companies having close family shareholdings or beneficial ownership
- e. Politically exposed persons (PEP) of foreign origin
- f. 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)
- g. Companies offering foreign exchange offerings
- h. 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.
- i. Non face to face clients
- j. Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and the company may exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

8. Customer Identification Procedures

Customer identification procedure means verifying the identity of the customer by using reliable, independent source documents, data or information. ASBPL needs to obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship. ASBPL must also be able to satisfy the regulators that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

- I. The Company shall duly comply with the KYC /client identification procedures that may be specified and strengthened by SEBI/FMC from time to time.
- II. 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.
- III. No business relationships can be established with PEP without the permission of the any one of the Director 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.
- IV. The concerned officials of the Company should track the financial soundness of the clients and shall take reasonable measures to verify source of funds of clients identified as PEP.
- V. The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the Company in compliance with the Guidelines.
- VI. The principal Officer shall ensure that the Client Identification Programme has been formulated and implemented as per the requirements of the Notification No. 9/2005 dated July 01, 2005 (as amended from time to time) and the PML Rules 2009.
- VII. It may be noted that while risk based approach may be adopted at the time of establishing business relationship with a client, no exemption from obtaining the minimum information/documents from clients as provided in the PMLA Rules is available to any class of investors with regard to the verification of the records of the identity of clients.
- VIII. There shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by the Company.

- IX. On failure by prospective client to provide satisfactory evidence of identity including address, financial status and the purpose of intended nature of relationship, new account shall not be opened and the matter shall be reported to the higher authority. This shall also apply where it is not possible to ascertain the identity of the client, or the information provided to the Company is suspected to be non genuine, or there is perceived non co- operation of the client in providing full and complete information.

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.

9. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. ASBPL can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity.

ASBPL shall have in place a comprehensive transaction monitoring process from a KYC/AML perspective. ASBPL shall put in place strong transaction alerts which will provide proactive signals on suspicious transactions and possible money laundering. ASBPL AML monitoring team shall endeavor to update the list based on current understanding of the market scenario and trading patterns followed by clients. In addition to the alerts from internal sources, the Surveillance & compliance team shall also monitor the alerts provided by the various exchanges.

On the basis of criticality of the breach, observation of account behaviour, repetitive breaches, the AML Monitoring Team shall send a query to the concerned Business. Responses would be expected within 7 working days. If the alerts still persist or the AML Monitoring Team is not satisfied with the responses, then the AML query team shall send the query to the Compliance Head for resolution.

In case of any account wherein alerts are observed on a regular basis, the risk categorization would be increased based on the consensus of the AML monitoring team and the compliance officer. Such a review would be done at least once every month.

Special attention is required for all complex, unusually large transactions / patterns which appear to have no economic purpose. The background including all documents, office records and clarifications pertaining to such transactions and their purpose will be examined carefully and findings will be recorded. Such findings, records and related documents would be made available to auditors and also to SEBI/FMC/Stock Exchanges/FIU-IND/Other relevant authorities, during audit, inspection or as and when required. These records to be preserved for ten years as required under PMLA 2002

It would be ensured that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority.

10. Risk Management

The overall responsibility/implementation and adherence of this shall lie with the Compliance, RMS & Surveillance Unit of ASBPL.

The Concurrent / Internal Auditors shall specifically check and verify the application of KYC/AML procedures and comment on the lapses observed in this regard. The reports and compliance in this regard shall also put up before the Audit & Compliance Committee of the Board at-least once in a quarter.

11. Combating Financing of Terrorism (CFT)

ASBPL shall have a heightened awareness in the system to check for transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism.

12. Maintenance of Records

In addition, the Principal Officer will ensure the maintenance of the following records:

- (i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- (ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
- (iii) 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;
- (iv) all suspicious transactions whether or not made in cash

Suspicious transaction means a transaction whether or not made in cash and including, inter-alia, credits or debits into or from any non monetary account such as demat account, security account etc. 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 bona .fide purpose;

A list of circumstances which may be in the nature of suspicious transactions is given

below. This 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:

- a) Clients whose identity verification seems difficult or clients that appear not to cooperate
- b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- c) Clients based in high risk jurisdictions;
- d) Substantial increases in business without apparent cause;
- e) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- f) Attempted transfer of investment proceeds to apparently unrelated third parties;
- g) Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export- import of small items.

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.

The Company shall also endeavour to maintain such records 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 to the investigating agencies for prosecution of criminal behavior. For this purpose we shall retain the documents as to

- (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. cash, cheques, etc.;
 - the identity of the person undertaking the transaction;
 - the destination of the funds;
 - the form of instruction and authority.

Principal Officer should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, he may consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI/FMC Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

13. Retention of Records

(a) The Company shall maintain necessary records on transactions, both domestic and international, at least for the minimum period prescribed under the SEBI/FMC Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

(b) 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 shall also be kept for the same period.

(c) In situations where the records relate to on-going investigations or transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 for the PML Rules, shall maintain at least for a period of Ten years from the date of the transaction or shall be retained until it is confirmed that the case has been closed.

14. Reporting to Financial Intelligence Unit-India

In terms of 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,
Chanakyapuri,
New Delhi-110021
Website: <http://fiuindia.gov.in>

For Cash Transaction Reporting (CTR)

Dealings in Cash, if any, requiring 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.

For Suspicious Transactions Reporting (STR)

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND within the required deadlines.

Where a client aborts/abandons a suspicious transaction on being asked some information by the company officials, the matter should be reported to FIU in the STR irrespective of the amount.

We will not base our decision on whether to file a STR solely on whether the transaction falls

above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal or terrorist corrupt activities.

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

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

No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported. We shall ensure not to put any restrictions on operations in the accounts where an STR has been made. ASBPL and its Directors, officers and employees (permanent and temporary) will be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. Thus, it should be ensured that there is no tipping off to the client at any level. Our company will create and maintain STRs and CTRs and relevant documentation on customer identity and verification. We will maintain STRs and their accompanying documentation for at least ten years.

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

We will adopt adequate screening procedures including background check to ensure high standards when hiring employees. Having regard to the risk of money laundering and terrorist financing and size of the business, the Company will identify the key positions and will ensure that the employees taking up such key positions are suitable and competent to perform their duties.

We will develop ongoing employee training under the leadership of the Principal Officer so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. They shall be made to fully understand the rationale behind this policy, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

We will develop in-house training in the company or outsource it. Means of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have hitherto never been called for, such as documents evidencing source of funds/income tax returns/bank records etc., which can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. Therefore, we will sensitize our customers about these requirements as the ones emanating from AML and CFT framework. We will prepare specific literature/ pamphlets etc./ hold conference so as to educate the customers of the objectives of the AML/CFT programme.

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. The Principal Officer accounts will be reviewed by the Directors.

Confidential Reporting of AML Non-Compliance:

Employees will report any violations of the company AML compliance program to the Principal Officer, unless the violations implicate the Principal Officer, in which case the employee shall report to the Board. Such reports will be confidential, and the employee will suffer no victimization for making them.

PERIODIC REVIEW OF THIS POLICY: The Board of Directors with competent authority will review and update the PMLA policy once in 2 years or as and when required and will be presented before the board in the board meeting.

COMMUNICATION OF THIS POLICY: Principal Officer shall ensure that this policy is communicated to all management and relevant staff including Directors, Head of the department (s), branches and group companies.

The company has made the PMLA policy which is informed to the Investors through the company's website and also carrying out Investor Education initiative by explaining the investors about the PMLA rules & requirements.

APPROVAL OF ODM COMMITTEE OF DIRECTORS

We have approved this revised AML program as reasonably designed to achieve and monitor our company ongoing compliance with the requirements of the PMLA and the implementing regulations under it. This Committee shall supervise the implementation of the AML Policy framework.

For ASNANI STOCK BROKER PRIVATE LIMITED



Authorized Signatory

(Policy updated/reviewed on – 10 July 2021)