Indbank Merchant Banking Services Limited

Policy Guidelines on Know Your Client (KYC) and Prevention of Anti Money Laundering (AML)

1. Preamble

1.1 Guidelines issued by SEBI

The Prevention of Money Laundering Act, 2002 (PMLA) was brought into force with effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on July 01, 2005by the Department of Revenue, Ministry of Finance, Government of India. As per the provisions of the PMLA, all securities market intermediaries registered under Section 12 of the SEBI Act, 1992 shall have to adhere to client account opening procedures and maintain records of such transactions as prescribed by the PMLA and rules notified there under. These guidelines were issued in the context of the amendments made to the PMLA and rules notified thereunder, updated guidelines in the context of recommendations made by the Financial Action Task Force (FATF) on anti-money laundering standards.

1.2 Anti Money Laundering Standards

Money laundering is the process whereby proceeds of crimes such as drug trafficking, smuggling, etc. are converted into legitimate money. The criminals attempt to hide and disguise the true origin and ownership of the proceeds of criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds. Thus money laundering is involvement in any transaction or series of transactions that seeks to conceal or disguise the nature or source of proceeds derived from illegal activities.

2. Objectives of Prevention of Money Laundering

2.1 The Anti Money Laundering Policy is to establish governing policies and standards to protect financial intermediaries from being used to launder money. The policy objectives are:

i. To protect the financial institutions including intermediaries from being used for money laundering
ii. To adhere to the statutory guidelines with regard to 'Know Your Customer' (KYC) policies and procedures
iii. To take appropriate action, once suspicious activity is detected and make report to the designated authorities in accordance with the applicable law/laid down procedures
iv. To comply with applicable laws as well as norms stipulated by the statutory authorities like NSE / BSE / SEBI etc.

2.2 As per the provisions of the PMLA, every banking company, financial institution (which includes chit fund company, a co-operative 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 market and registered under Section 12 of the SEBI Act , shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include;

a) All cash transactions of value of more than Rs.10.00 lakhs or its equivalent in foreign currency.

b) All series of cash transactions integrally connected to each other which have been valued below Rs.10.00 lakhs or its equivalent in foreign currency where such series of transactions taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency

c) All suspicious transactions whether or not made in cash and including, inter-alia, credit or debits into from any non monetary account such as de-mat account, security account maintained by the registered intermediary.

It is also clarified that for the purpose of suspicious transactions reporting apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.

3. KYC Guidelines - A Tool to Prevent Money Laundering

Know Your Customer (KYC) guidelines are important tools to ensure that the financial system is not used for laundering proceeds of criminal activities. KYC norms/guidelines play a very important role in preventing money laundering.

As per SEBI circular dated 10.11.2016 on uploading of existing clients KYC details with central KYC record registry system by the registered intermediaries, company has got itself registered as an entity with CERSAI and has resolved to comply with various guidelines given by CERSAI for updation of CKYCR within time line and shall remain compliant by uploading KYC records to CKYCR with CERSAI directly.

To meet the regulatory requirements and to guide the field level functionaries of the companies, it was decided to frame comprehensive Policy guidelines on Prevention of Anti Money Laundering. Accordingly thisPolicy guidelines are prepared for information, guidance and implementation.

3.1 Company's detailed KYC Policy:

Who is a Customer?

For the purpose of KYC policy, a 'Customer' is beneficiary of transactions conducted by professional intermediaries, such as Stock Brokers etc., as permitted under the law.

3.2 Objectives

The main objective of KYC guidelines is to prevent the company from beingused**,** intentionally or unintentionally, by criminal elements for money laundering activities.

Know Your Customer is the principle on which the company operates to avoid the pitfalls of operational, legal and reputation risks and consequential losses by scrupulously adhering to the various procedures laid down for opening and conduct of accounts.

The KYC guidelines go beyond merely establishing the identity of the person. The due diligence expected under KYC involves going in to the purpose and reasons for opening*the account***,** anticipated turnover in the account, source of wealth (net worth)of the person opening the account and sources of funds flowing into the account. Thus, this is not a responsibility, which ends with the opening of the account. Ongoing monitoringis an essential element of effective KYC procedures.

3.3 Other objectives in stipulating KYC guidelines are:

- To minimize frauds
- To check misappropriations
- To weed out undesirable customers

- To Prevent Money Laundering
- To avoid opening of accounts in anonymous or benami/ fictitious names and addresses

4. Need for Policies and Procedures to Combat Money Laundering and Terrorist financing

International initiatives taken to combat drug trafficking, terrorism and other organized and serious crimes have concluded that financial institutions including securities market intermediaries must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing. The said obligation on intermediaries has also been obligated under the Prevention of Money Laundering Act, 2002. In order to fulfill these requirements, there is also a need for registered intermediaries to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

4.1 Prevention of Money Laundering Policy of the company contains the following aspects:

a) Policies and procedures, on a group basis wherever applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;

(b)The Policy is drafted in such a way that the content of these Guidelines are understood by all staff members;

(c) The Policy laid down is subject to review by the competent authority from time to time as per the guidelines issued by the statutory authorities from time to time.

(d) Customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing;

(e) Customer due diligence ("CDD") measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction.

(f)Place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and

(g) develop staff members' awareness and vigilance to guard against money laundering and terrorist financing.

4.2 The Policy and procedure to combat Money laundering covers:

a. Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or Registered Office;

b. Customer acceptance policy and customer due diligence measures, including requirements for proper identification;

c. Maintenance of records;

d. Compliance with relevant statutory and regulatory requirements;

e. Co-operation with the relevant law enforcement authorities, including the timely

disclosure of information; and

f. Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors

4.3 Salient Features of Revised Policy

In order to achieve the objectives of Anti Money Laundering guidelines by the statutory authorities, under the overall "Client Due Diligence Process" the following three key elements have been made.

i. Policy for acceptance of clients**(Appendix I)**
ii. Procedure for identifying the clients**(Appendix II)**
iii. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)**(Appendix III)**

4.4 The salient features of the company's revised KYC policy and Anti Money Laundering Standards are summarised below:

a. Policy for acceptance ofClientshas been framed as part of KYC policy
b. Parameters of risk perception for customers have been defined based on whichcustomers are to be categorized
c. Preparation of a profile for each customer based on the risk categorisation
d. Fixing of threshold limit for each account (based on risk perception) to have effectivemonitoring
e. Procedure for identifying clients have been spelt out for different types ofcustomers and the documents/information to be obtained have been dealt in detail
f. Guidelines for Transaction *monitoring and Suspicious Transactions Reporting(STR)*.
h. Appointment of Principal Officer for the company for monitoring and reporting of identified / suspicious transactions and sharing information as required under the law.

5. Obligation to Maintain Secrecy of Information Received

Terminals should treat the information collected from the customer for the purpose of opening of account as confidential and not divulge any details thereof either for cross selling or for any other purposes./Terminals shall therefore, ensure that information sought from the customer under KYCnorms

i. is relevant to the perceived risk
ii. is ***not*** intrusive
iii. is in conformity with the guidelines issued by the company from time to time in this regard.

6. Record Keeping

As per the master circular issued by SEBI on prevention of Money Laundering the registered intermediary should 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 for prosecution of criminal behavior.

Should 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, we should retain the following information for the accounts of the 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, Demand drafts etc.:
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

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

More specifically, the following records, as prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002, are to be maintained by service branchwhere all the operations of the company is centralized, for a period of FIVE YEARS.

(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 exceed rupees ten lakh or its equivalent in foreign currency;
(iii) 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.

7. Information to be Maintained:

The following informations are to be maintained as referred to in Rule 3 of PMLA Rules:
I. the nature of the transactions;
II. the amount of the transaction and the currency in which it denominated;
III. the date on which the transaction was conducted; and
IV. the parties to the transaction.

These records to be maintained and preserved by the Service branch for a period of five years from the date of transactions between the client and IBMBS.

The records evidencing the identity of the clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved by Service branch for a period of five years after the business relationship between a client and intermediary

has ended or the account has been closed, whichever is later.

8. The following are the document retention terms:

(a) All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

(b) Service branch to maintain and preserve the record of documents evidencing the identity of all clients and beneficial owners (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 for a period of five years after the business relationship between a client and the company has ended or the account has been closed, whichever is later

c) In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

9. Records of information reported to the Director, Financial Intelligence Unit – India (FIU – IND): Service branch to maintain and preserve the 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, for a period of five years from the date of the transaction between the client and the company.

10. KYC for the existing accounts

The revised guidelines will apply to all new customers and to the existing customers on the basis of materiality and risk. All the existing accounts of companies, trusts, and other institutions shall be subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'. However, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the Customer Due Diligence measures.

11. Non co-operation, Non submission of documents/data/information by customer

In respect of existing accounts, where the branch/terminal is not able to apply KYC norms especially in monitoring of transactions due to non co-operation by the customer, or non reliability of the data/information furnished to the company, branch/terminal may stop the operations forthwith.

12. Principal Officer

Vice President & Company Secretary or such other officer nominated by the President of the company shall be theauthority to ensure the effective implementation of Company's KYC policy and Anti Money Laundering measures by branches. He shallexplicitly allocate duties and responsibilities for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective accounts. It should cover proper management oversight, systems and controls and other related matters. the Principal Officer shall 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 and shall have access to and be able to report to senior management at the next

reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU. The Compliance of instructions/guidelines issued by SEBI/NSE/BSE from time to time is to be reported to all branches by the Principal Officer

TerminalIn Charges/Service Branch Head shall be responsible for ensuring that company's policies and procedures are implemented in letter and spirit and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective accounts.

13. **Designated Director**

President & Whole Time Director will be the Designated Director, who will ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules. In terms of Section 13 (2) of the PML Act (as amended by the Prevention of Money-laundering (Amendment) Act, 2012), the Director, FIU-IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations. The principal officer shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

14. Employees' Hiring/Employee's Training/ Investor Education

a. Hiring of Employees:

The company shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

b. Employees' Training:

The company must have an ongoing employee training programme at least once in a financial year 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. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

c. Investors Education:

Implementation of AML/CFT measures requires the company to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need for the company to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Thecompanyshall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

15. Role of Internal Auditor:

Internal audit should cover in their report as to whether the policies and guidelines framed by the company in line with the SEBI guidelines are being followed or not. The report shall also cover the compliance requirement of relevant statutory and regulatory authorities and Co-operation with the relevant law enforcement authorities including the timely disclosure of information.

Appendix – I

Policy for acceptance of clients

The client acceptance policies and procedures of the company aims to identify the types of clients that are likely to pose a higher than average risk of ML or TF. By establishing such policies and procedures, thecompany 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 transaction. In a nutshell, the following safeguards will be followed while accepting the clients:

a) No account is opened in a fictitious / benami name or on an anonymous basis.

b) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly 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 higher degree of due diligence and regular update of Know Your Client (KYC) profile.

c) Documentation requirements and other information to 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.

d) Ensure that an account is not opened where the company is unable to apply appropriate CDD measures/ KYC policies. This shall apply in cases 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. The company shall not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The company shall be cautious to ensure that it does not return securities of money that may be from suspicious trades. However, The Company shall consult therelevant authorities in determining what action it shall take when it suspects suspicious trading.

e) The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons i.e. the agent- client registered with the company, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

f) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known

criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide

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

1. **Categorisation**of**customers**

As regards categorisation based on risk perception, customers are to be categorised into threelevels as under:

Low Risk Customers
Medium Risk Customers
High Risk Customers

2.1 Low Risk Customers

The following category of clients will fall under this category:

Individuals (other than High Net Worth)andentitiesopeningStock broking and/orDemat*account*whose identities and sources ofwealth can be easily identified and transactions in whose accounts by and large conform to theknown profile, are to be categorised as low risk customers

Illustrative examples oflow risk customers are:

i. Salaried employees whose salary structures are well defined, Pensioners
ii. People belonging to lower economic strata of the society whose accounts showsmall balances and low turnover
iii. Individuals whose Networth / Holdings value from known sources does not exceed Rs.10Lakhs

2.2 Medium Risk Customers

Customers that are likely to pose a slightly more than average risk to the company are to be categorized as medium risk customers (Category II).
Illustrative examples are:

i.High Networth Individuals. For this purpose an individual is considered as HighNetworth whose Networth / Holdings value from known sources is above Rs.10.00 lakhs and upto Rs.2 Crores.
ii. NRI Customers
iii.Corporate Customers
iv.Accounts of individuals operated by a Mandate or Power of Attorney Holder
v. Companies (both Private and Public), with *annual turnover up to Rs. 5 Crores*
vi.Accounts of Trusts / HUF

Under this category, terminals should apply enhanced Customer Due Diligence (CDD) while opening accounts.Terminals shall call for *additional* information and documentary evidence, besides the normal documents prescribed for low risk customers

2.3 High Risk Customers:

Customers that are likely to pose a high degree of risk to the company are to be categorizedas high risk customers (Category III). Examples of this type of customers are:

a. HighNetworthIndividuals,withNetworth / Holdings valuefromknownsourcesisaboveRs.2 Crores.

b. Trusts, Charities, NGOs and organisations receiving donations
c. Politically Exposed Persons (PEPs) of foreign origin
d. Non-face to face customers
e. Clients with dubious reputation as per public information available
f. Companies offering foreign exchange offerings
g. 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)
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. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information
i. All other accounts/entities that could not be categorised under Low and/or Medium Risk.

Terminals should apply *intensive* Customer Due Diligence (CDD) while openingaccounts of High Risk Customers especially those for whom the sources of funds are notclear.

2. Non co-operation, Non submission of documents / data / information by customer

Where the terminal is unable to apply appropriate customer due diligence measures i.e. terminal is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non co-operation of the customer or non reliability of the data/information furnished to the company, the terminal may take a decision not to open the account.

3. Risk-based Approach:

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. As such, the company shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the company shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, 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 the company shall obtain necessarily depend on the risk category of a particular client.

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

4. Risk Assessment:

a) The company shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its

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 thevarious United Nations' Security Council Resolutions. These can be accessed at the URL

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and
http://www.un.org/sc/committees/1988/list.shtml

b) The risk assessment carried out shall 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.

5. The following risk assessment measures are to be carried out by Service branch, Chennai

1. Records of Individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council, availablein URL:
   http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and
   http://www.un.org/sc/committees/1988/list.shtml
   to be preserved.The records need to be updated based on issuance of Press release documenting changes in the list & posted in the "Press releases" section and circulated by the Exchanges and DP.
2. While opening demat and trading accounts for our customers, it must be ensured that accounts are not opened for entities included in the above list.

Appendix II

Client Identification Procedures

1. To achieve the objectives of the KYC framework that is

(i) to ensure appropriate customer identification and
(ii) to monitor transactions of a suspicious nature

Terminals should obtain all information necessary to establish the identity/legal existence of each new customer, based preferably on disclosures by customers themselves.

The KYC policy shall clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the client relationship, while carrying out transactions for the client or when the company has doubts regarding the veracity or the adequacy of previously obtained client identification data.

The company shall be in compliance with the following requirements while putting in place a Client Identification Procedure (CIP):

a) The company shall proactively put in place appropriate risk management systems to determine whether its existing client or potential client or the beneficial owner of such 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. Further, the enhanced CDD measures shall also be applicable where the beneficial owner of a client is a PEP.

b) Senior management approval would 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, the company shall obtain approval from senior management to continue the business relationship.

c) The company shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

d) The client shall be identified by the company by using reliable sources including documents / information. the company shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

e) The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the company in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the Principal Officerof the company.

SEBI has prescribed the minimum requirements relating to KYC from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, the company shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.Further, the company shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued there under so that the

company is aware of the clients on whose behalf it is dealing.

The company shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients and such other additional requirements that it considers appropriate to enable the company to determine the true identity of its clients.

It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to the company from obtaining the minimum information/documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by the company. This shall be strictly implemented by the company.

2. Reliance on third party for carrying out Client Due Diligence (CDD)

2.1The company 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 party 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.

2.2 Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the company shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

3. Client Due Diligence (CDD)

The CDD measures at the company shall comprise the following:

a) Obtaining 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. 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) Verifying the client's identity using reliable, independent source documents, data or information.

c) Identifying 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.

i. For clients other than individuals or trusts

Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the company shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

aa) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.
Explanation: Controlling ownership interest means ownership of/entitlement to:

i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;

ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

bb) In cases where there exists doubt under clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.
Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

ii. For client which is a trust:
Where the client is a trust, the company shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

iii. Exemption in case of listed companies:
Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it will not be necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

iv. Applicability for foreign investors
While dealing with foreign investors, the company will be guided by the clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.

d) Verifying 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) Understanding the ownership and control structure of the client.

f) Conducting 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's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds

4. Periodic Updation of KYC Documents

Thecompanyshall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such periodicity of KYC updation shall be based on the risk profile of the customer. Periodic updation of KYC shall be carried out

- At least once in every two years for high risk customers
- Once in every eight years for medium risk customers
- Once in every ten years for low risk customers

taking in to account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained. Physical presence of the clients may, however, not be insisted upon at the time of such periodic updations.

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 in respect of any class of investors with regard to the verification of the records of the identity of clients.

5. Account Opening for clients

a. Low Risk Category

In respect of Account opening for Broking and DPfor individuals under low risk category, terminals shall be required to verify the following documents which may be accepted for identification and location:

1) PAN Card (Xerox Copy) Compulsory (Self attested by the Client)
2) Any one of the following documents for ID Proof and Address Proof (Self attested by the Client):

ID Proof	Address Proof
1. Passport	1. Passport
2. Voter's Identity Card	2. Voter ID
3. Photo Identity Card issued by Govt/PSU	3. Driving License
4. Aadhaar Card	4. Bank Account Statement/Passbook Not more than 3 months old
5. Driving License	5. Ration Card
	6. Aadhaar Card
	7. Insurance Premium Receipt
	8. Flat Maintenance Bill
	9. Registered Lease or Sale agreement of Residence

	10. Utility Bills like Telephone Bill, Gas Bill,Electricity Bill not more than 3 Months old. old.

Note: Original should be produced for verification and copy, duly attested by the verifying official, should be kept along with the account opening form.

The documents listed above are only illustrative based on the list provided by regulatory authorities. Addition/Deletion/Modification to the list by the regulators, depending on subsequent developments may be accepted for identification and location from time to time.

When the aforesaid documents are accepted as the basis for opening theStock broking and Demataccountin the name of the holder of such document(s), the officerauthorising the opening of such account must

i. verify that the documents are prima facie in order.

ii. ensure that the passports, identification cards, etc., are valid and are not out of date.

iii. ensure that the signatures of the applicant and other particulars as given on the application form agrees with the signature and other particulars recorded in the above cited documents and appearance of the applicant also agrees with the photograph on the passport and/or other documents to his/her satisfaction.

iv. note all the relevant particulars such as reference number, authority, date and place of issue, etc. of passport, voter's identity card, driving license etc., in the account opening form in the introduction columns.

v. authenticatedcopies of the documents shall be obtained and keep along with the account opening form.

vi. In-person verification shall be carried out certifying the documents with reference to the originals

vii. Required number of Photographs of the customers should be obtained and maintained.In case of closure of accounts the photographs should not be returned to the clients.

b. Medium / High Risk Customers

In respect of medium/high risk customers, terminals shall call for ***additional*** information and documentary evidence, (besides the normal documents prescribed above) which may include

Type of Customers/accounts	**Additional Information/Documents**
i. For opening Non Resident accounts	Passport

ii. For opening accounts of other than NRIs under Medium and High Risk categories iii.For current accounts in all risk categories iv. For accounts of other than individuals in all risk categories	In addition to obtention of documents/ information for identity and location of the customer, introduction may be obtained

For customers that are legal persons or entities (i.e., other than individuals), branches should:

- verify the legal status of the legal person/entity through proper and relevant documents

- verify that any person(s) purporting to act on behalf of the legal person/entity is duly authorized and such person(s) is/are properly identified by calling for documents (as listed above for individual low risk customers) and verify the identity of that person(s)

- understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person

If business or residential address of the prospective account holder is outside the area ofoperation of the terminal or if the introducer is an account holder of another branch/terminalproperenquiries should be made about the reason for opening of the account.TheTerminal Head has to make more enquiries than usual to test the credentials of theprospective customer before allowing him/her toopen the account.

6. **Dispatch of Account Opening intimation to new customers**

Service Branch will send theAccount Opening Intimation to all Stock broking / Demat account customers in a closed cover.

In cases where Account Opening Intimation letters are returned undelivered for the reasons *"No suchaddress, No such person/addressee"* and alike,

i. 'Caution' should be noted in the Account and intimation to be given to the concerned branch/terminal.

ii.Terminal Head/any other officer of the terminalshouldcall at the address given in the account opening form to verify whether the reason for non-delivery is correct.

When it is established beyond doubt that the account was opened in fictitious name andAddress a report should be sent to the Principal Officer immediately.

Appendix – III

Monitoring of Transactions

1. <u>Monitoring of transactions</u>

Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the company has an understanding of the normal activity of the client so that it can identify deviations in transactions / activities.

The company shall pay special attention to all complex unusually large transactions /

patterns which appear to have no economic purpose. the company may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. 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/FIUIND/ other relevant Authorities, during audit, inspection or as and when required. These records will be maintained and preserved for a period of five years from the date of transaction between the clients and the company.

The company shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and the transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities (Director) within the company.

Further, the compliance cell of the company shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

All regulatory alerts generated by the Market Infrastructure Institutions (MIIs) shall be monitored by the Principal Officer for necessary action to be taken

2. Suspicious Transaction Monitoring and Reporting

The company shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, the company shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

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.

Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer (Principal Officer) or any other designated officer within the company. 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. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Principal Officer/ Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that the company shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

The clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC'. Such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

3. **High Value Transaction:**

A list of transactions which may be classified as high value transactions is given below.

a) Under DP single transaction involving more than 25000 shares by quantity and / or Rs.5lakhs in value.
b) Under Stock broking single transaction of value of Rs.10.00 lakhs and above.
c) Transaction in pennyscrips(illiquid stocks notified by exchanges from time to time) when the total value of the transaction is above Rs.5.00 lakhs and or the number of shares transacted is above 1000.

Any suspicion / high valuetransaction should be immediately notified to the Principal Officer with details of the clients, transactions and thenature /reason of suspicion, by the branches/terminals/service branch. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that branches/terminals should report all such attempted transactions to Principal Officer, even if not completed by customers, irrespective of the amount of the transaction.

4.Internal Control Systems:

Necessary provisions shall be made in the respective software for identifying and generating reports of High Value Transactions for monitoring under the guidelines.

This report shall be generated, reviewed and reported by the officer in charge of service branch on a weekly basis in the MIS report placed to the management.

5. List of Designated Individuals/ 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. The company shall ensure that accounts are not opened in the name of anyone whose name appears in said list. The company shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts

bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

6. Procedure for freezing of funds, financial assets or economic resources or related services

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA.

Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

The company shall ensure effective and expeditious implementation of the procedure laid down in the UAPA Order dated August 27, 2009 as listed below:

a) On receipt of the updated list of individuals/ entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/ entities)fromthe Ministry of External Affairs (MHA)' and forwarded by SEBI, the company shall take the followings steps:

i. The company will maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

ii. In the event, particulars of any of customer/s match the particulars of designated individuals/entities, the company shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

iii. The company shall send the particulars of the communication mentioned in (ii) above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, BandraKurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND.

iv. In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, the company would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on

011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

v. The company shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above carried through or attempted, as per the prescribed format.

b) On receipt of the particulars as mentioned in paragraph (ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by the company are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by the company are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

c) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section51A of the UAPA would be issued within 24 hours of suchverification and conveyed electronically to the concerned depository under intimation to SEBI and FIU-IND. The order shall take place without prior notice to the designated individuals/entities.

d) Implementation of requests received from foreign countries under U.N. Securities Council Resolution 1373 of 2001.

i. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

ii. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

iii. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officer in SEBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

iv. Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to the company and the procedure as enumerated at paragraphs (a) and (b) shall be followed.

v. The freezing orders shall take place without prior notice to the designated persons involved.

e) Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

i. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the company. The company shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 5 above within twoworking days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock exchanges, depositories and the company. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

f) Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

i. All Orders under section 51A of the UAPA relating to funds, financial assets or economic resources or related services, would be communicated to stock exchanges, depositories and the company through SEBI.

7. Reporting to Financial Intelligence Unit-India

In terms of the PML Rules, the company 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

The company shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND under the Section Obligation of Reporting Entity – Furnishing Information – Reporting Format (https://fiuindia.gov.in/files/downloads/Filing_Information.html). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents While detailed instructions for filing all types of reports are given in the instructions part of the related formats, the company shall adhere to the following:

a) The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

b) The Suspicious Transaction Report (STR) shall be submitted 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 his reasons for treating any transaction or a seriesof transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

c) The Non Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

d) The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

e) Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.

f) No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.

The company shall not put any restrictions on operations in the accounts where an STR has been made. The company and its directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level. It is clarified that the the company, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if the company has reasonable grounds to believe that the transactions involve proceeds of crime.

8. Modification and Review:

The Policy guidelines shall be reviewed by the President, once a year and modified if necessary to suit the needs of the company and to comply with the regulatory requirements from time to time.

Designated Director: Shri. Haribabu V

Principal Officer: Shri. TausifInamdar

This policy was reviewed by the Board of Directors of the Company in their Meeting held on 28.03.2022.