

PMLA Policy

Kimaya Securities and Financial
Services Pvt. Ltd.

10/30/2024



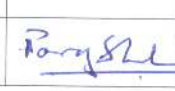
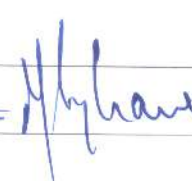
Contents

<i>Document Control Page</i>	4
<i>Scope/ Applicability</i>	5
<i>Background</i>	7
<i>Essential Principles</i>	7
<i>Obligation to establish policies and procedures</i>	8
<i>Written Anti Money Laundering Procedures</i>	8
<i>Policy</i>	9
1.0 Policy Guidelines on 'Know Your Customer' norms And Anti-Money Laundering measures	9
2.0 Definition of Money Laundering	9
3.0 Obligations under Prevention of Money Laundering [PML] act 2002	9
4.0 Policy Objectives	10
5.0 Scope	10
6.0 Client Due Diligence (CDD)	10
I. Client acceptance policy	11
II. Client identification procedure	12
III. Reliance on third party for carrying out CDD	13
IV. Risk management	14
i. Risk based approach	14
ii. Risk assessment and categorization	14
V. Monitoring of transactions	17
7.0 Suspicious transaction monitoring and reporting	18
8.0 Information to be maintained	19
9.0 Record Keeping	19
10.0 Retention of Records	20
11.0 Procedure for freezing of funds, financial assets or economic resources or related services	21

12.0	Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries.....	21
13.0	List of Designated Individuals/ Entities:.....	22
14.0	Jurisdictions that do not or insufficiently apply the FATF Recommendations.....	23
15.0	Reporting to Financial Intelligence Unit-India (FIU IND).....	23
16.0	Designation of officers for ensuring compliance with provisions of PMLA.....	25
17.0	AML Team.....	26
18.0	Hiring of Employees and their Training.....	26
19.0	Investors Education.....	27
20.0	Review of the Policy.....	27
	Annexure- I: Customer Identification Requirements – Indicative Guidelines.....	28

Document Control Page

Document Name	PMLA Compliance Policy
Applicability	Stock Broking Services

Authorization	Document Owner	Drafted by	Last Reviewed On	Reviewed by	Authorized by
Mr Nikunj Singhania	Kimaya Securities and Financial Services Pvt. Ltd.	Mr Kamlesh Modi	30-10-2024	Mr Parag Shah	Mr Nikunj Singhania
					

Classification	Distribution List
Official Use Only	Employees of the Company / Branch Heads

All queries, suggestions and changes required may be emailed paraghshah9@kimayasecurities.com (Principal Officer).

The information contained in this document is CONFIDENTIAL and may be legally PRIVILEGED. Any disclosure, copying, distribution, dissemination, forwarding, printing or any action taken in reliance on it or utilizing the same for any purpose other than what it is intended for, without consulting the **Kimaya Securities and Financial Services Pvt. Ltd.** is prohibited and may be unlawful.

Scope/ Applicability

PROVISION	RESPONSIBLE DEPARTMENT	ACTION
<p>Customer Due Diligence Policy for acceptance of clients:</p> <p>Clients of special category (CSC):</p> <p>Client identification procedure :</p>	Customer care / Compliance Department	<p>Customer care department with the co-ordination of compliance department will take care of customer due diligence. Client should be categorized into high risk, moderate & low risk.</p> <p>Customer Due Diligence by Third party shall be permitted as an exception only and with approval of the Board.</p>
Record Keeping	Finance & Accounts	Cash transactions, if any shall be permitted only as per extant guidelines. Record to be maintained of all Cash transactions above Rs. 10 lakhs. Record of all transactions including suspicious transactions to be maintained in hard / soft copies.
Retention of Records	All Departments.	Records to be maintained for 5 years.
Monitoring of transactions	Compliance Department	All alerts shall be scrutinized and suspicious transactions shall be escalated to the principal officer. The principal officer shall take immediate action on all such transaction and report it to FIU IND, in case the client is unable to provide necessary information as to the genuineness of the transaction.
Suspicious Transaction Monitoring & Reporting	Principal Officer	<p>Record to be maintained of payments or transfers received from third parties (other than clients) which are of suspicious nature, if any.</p> <p>Record is to be maintained for transfers which are of suspicious transactions in the client accounts.</p>
Designation of an officer for reporting of suspicious transactions	Management & Board of Directors	Board of Directors will appoint principal officer and will intimate to FIU-India, New Delhi
Designation of an Director for reporting of suspicious transactions by Principal	Management & Board of Directors	Board of Directors will appoint Director and will intimate to FIU-India, New Delhi

Officer		
Furnishing of information to the Director (FIU)	All Departments.	<p>The Principal Officer shall furnish the information in respect of transactions referred to in rule 3 every month to the Designated Director by the 15th day of the succeeding month. 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.</p> <p>No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported</p>

Background

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, 2005 by the Department of Revenue, Ministry of Finance, Government of India.

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:

- i. All cash transactions of the value of more than Rs. 10 lakh or its equivalent in foreign currency.
- ii. All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees 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.

For the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.

Essential Principles

- If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups shall be required to apply appropriate additional measures to manage the ML/TF risks, and inform SEBI.
- In case there is a variance in Client Due Diligence (CDD)/ Anti Money Laundering (AML) standards specified by SEBI and the regulators of the host country, branches/overseas subsidiaries of the RE shall adopt the more stringent requirements of the two.
- This Policy only supplements the existing SEBI / FIU guidelines relating to KYC/AML and any subsequent guidelines from the date of the Policy on KYC/AML will be implemented immediately, with subsequent ratification by the Board. Extant regulations will at any point in time override this Policy.

Obligation to establish policies and procedures

- Group: "group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of Rule 2 of the PML Rules as amended from time to time. Groups shall implement group-wide policies for the purpose of discharging obligations under Chapter IV of the PMLA.
- Financial groups must implement programs applicable to all branches and majority-owned subsidiaries.
- These programs include policies and procedures for sharing information related to customer due diligence (CDD) and ML/TF risk management.
- Group-level compliance, audit as applicable as per Regulatory requirements and AML/CFT functions should provide necessary customer, account, and transaction information.
- Adequate safeguards must be in place to protect confidentiality and prevent tipping-off.
- The senior management of the RE shall establish appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The RE shall:
 - issue and implement policies and procedures reflecting current requirements (on a group basis, if applicable)
 - ensure that the same is understood by the staff
 - review policies and procedures on a regular basis
 - adopt client acceptance policies sensitive to ML and TF risks
 - undertake CDD measures based on client type, business relationship, or transaction
 - establish a system for identifying, monitoring, and reporting suspected ML or TF transactions to law enforcement
 - develop staff awareness and vigilance to prevent ML/TF
- Policies and procedures to combat ML/TF shall cover:
 - Communication of group policies to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries
 - Client acceptance, identification and CDD measures
 - Maintenance of records
 - Compliance with relevant legal requirements and co-operation with relevant law enforcement authorities
 - Role of internal audit or compliance function as applicable under regulatory requirements

Written Anti Money Laundering Procedures

The RE shall adopt the following 'Client Due Diligence' procedures as specified in the policy:

- i. Policy for acceptance of clients;
- ii. Procedure for identifying the clients;
- iii. Risk Management;
- iv. Monitoring of Transactions

Policy

1.0 Policy Guidelines on 'Know Your Customer' norms And Anti-Money Laundering measures

In terms of the guidelines issued by the Securities Exchange Board of India (SEBI) on Know Your Customer (KYC) standards and Anti Money Laundering (AML) measures, intermediaries are required to put in place a comprehensive policy frame work covering KYC Standards and AML Measures.

For the purpose of this policy, the Kimaya Securities and Financial Services Pvt. Ltd. shall be referred as the Reporting Entity or RE.

Accordingly, this policy document is prepared in line with the SEBI guidelines regarding customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis. The objective of this policy document is to prevent the RE from being used, intentionally or unintentionally, by criminal elements for money laundering activities and for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

2.0 Definition of Money Laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the “offence of money laundering” as under:

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

Money launders may use the system for clearing ‘money’ earned through criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds. Money launders also disguise the true source of funds by investing the funds earned out of terrorist / criminal activities through third party accounts.

3.0 Obligations under Prevention of Money Laundering [PML] act 2002

Section 12 of PML Act 2002 places certain obligations on every banking company, financial institution and intermediary which include:

- a. maintaining a record of prescribed transactions
- b. Furnishing information of prescribed transactions to the specified authority
- c. Verifying and maintaining records of the identity of its clients
- d. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF
- e. develop staff members’ awareness and vigilance to guard against ML and TF

4.0 Policy Objectives

- a. To prevent criminal elements from using the RE's system for money laundering activities.
- b. To enable the RE to know / understand its customers and their financial dealings better, which in turn would help the RE to manage risks prudently.
- c. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- d. To comply with applicable laws and regulatory guidelines related to anti - money laundering.
- e. To take necessary steps to ensure that the concerned staff are adequately trained in KYC/AML procedures.

5.0 Scope

This policy is applicable to all branches/offices of the RE and is to be read in conjunction with related operational guidelines issued from time to time.

6.0 Client Due Diligence (CDD)

The following CDD measures shall be taken by the RE:

- a) The RE shall obtain sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. 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 client's identity using reliable, independent source documents, data or information. Obtain information on the purpose and intended nature of business relationship, where applicable. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person
 Provided that in case of a Trust, the reporting entity shall ensure that trustees disclose their status at the time of commencement of an account based relationship.
- c) The RE shall 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. The guidelines for the identification of beneficial ownership. Refer policy on Identification of Beneficial Ownership.
- d) The RE shall 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 (b).
- e) The RE shall understand the nature of business, the ownership and control structure of the client.
- f) The RE shall conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

- g) The RE shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data.
- h) The RE shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients
- i) Every RE shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later
- j) Where RE is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND.
- k) The RE shall not undertake any transaction or account-based relationship without following the CDD procedure.

The Client due Diligence Process includes the following specific parameters:

- I. Client acceptance policy
- II. Client Identification procedure
- III. Reliance on third party for carrying out Client Due Diligence (CDD)
- IV. Risk assessment
- V. Monitoring and reporting of transactions

I. Client acceptance policy

The following client acceptance policy indicating the criteria for acceptance of customers shall be followed in by the RE. The staff shall accept client strictly in accordance with the said policy:

- a) No account shall be 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 shall be 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 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) The staff shall collect documents and other information 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) Account shall not opened where the intermediary is unable to apply appropriate CDD measures / KYC policies. This is applicable in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is

suspected to be non-genuine, or there is perceived non co-operation of the client in providing full and complete information. The RE shall not continue to do business with such a person and shall file a suspicious activity report. It shall also evaluate whether there are suspicious transactions in determining whether to freeze or close the account. The RE shall be cautious to ensure that it does not return securities or money that may be from suspicious transactions. However, the RE shall consult the relevant 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 is specified in what manner the account are 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 intermediary, as well as the person on whose behalf the agent is acting are clearly laid down. Adequate verification of a person's authority to act on behalf of the client is carried out.
- f) The staff shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. SEBI has been circulating lists of terrorist entities notified by the UNSC/Government of India so that the RE exercise caution against any transaction detected with such entities. The staff shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the RE are not in any way involved in any unlawful activity and that they do not appear in such lists.
- g) The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

II. Client identification procedure

1. Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information.
2. The staff shall independently obtain sufficient and reliable documents information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship. Each original document is seen prior to acceptance of a copy. Being satisfied means that the staff member is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For clients that are natural persons, the staff shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For clients that are legal persons or entities, the staff shall (i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Client Identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure-I.

3. If the staff member decides to accept such accounts in terms of the Customer Acceptance Policy, the staff member shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. Refer policy on Identification of Beneficial Ownership.
4. Due diligence should be carried out to ensure that no account is opened in a fictitious/ Benami name or anonymous basis and also verified with the UN list of banned entity, SEBI banned entity list or orders/investigations issued by regulatory authorities/media information.
5. The staff shall obtain information about the client as per the requirement mentioned in the Account Opening Form for the different categories of clients.
6. Failure by prospective client to provide satisfactory evidence of identity are noted and reported to the higher authority within the intermediary.
7. The staff shall obtain senior management approval 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 staff shall obtain senior management approval to continue the business relationship. The RE shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
8. There are no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by the RE.
9. The RE shall update documents, data or information of dormant clients whenever the account is re-activated by the client as per regulatory guidelines.
10. The RE 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 thereunder so that the RE is aware of the clients on whose behalf it is dealing.
11. The RE shall follow the client identification and KYC/account opening procedures and guidelines prescribed by SEBI and other regulatory authorities. The Board of the RE may, if required, frame policy for the same.
12. The RE shall incorporate the requirements of Rule 9 of the PML Rules as updated from time to time in the Client Identification procedure.

III. Reliance on third party for carrying out CDD

The RE may rely on 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.

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. In terms of Rule 9(2) of PML Rules:

- i. The RE shall immediately obtain necessary information of such client due diligence carried out by the third party;
- ii. The RE shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- iii. The RE shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
- iv. The third party is not based in a country or jurisdiction assessed as high risk;
- v. The RE shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

IV. Risk management

i. Risk based approach

Certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. The RE shall apply each of the client due diligence measures on a risk sensitive basis. The RE shall adopt an enhanced client due diligence process for higher risk categories of clients. 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 RE shall obtain necessarily depend on the risk category of a particular client. 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.

ii. Risk assessment and categorization

1. The staff shall prepare a profile for each new customer based on risk categorization. The RE has devised a Composite Account Opening Form for recording and maintaining the profile of each new customer. The form is separate for Individuals, Partnership Firms, Corporate and other legal entities, etc. The nature and extent of due diligence shall depend on the risk perceived by the staff member. The staff shall continue to follow strictly the instructions issued by the RE regarding secrecy of customer information. The staff should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of services to general public, especially to those, who are financially or socially disadvantaged.

2. The RE 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. Risk assessment on money laundering is dependent on kind of customers the Company deals with. Typically, risks are increased if the money launderer can hide behind corporate structures such as limited companies, offshore trusts, special purpose vehicles and nominee arrangements.
3. The RE shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries shall ensure:
 - To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
 - Adoption of a risk-based approach to manage and mitigate the risks".
4. The risk assessment shall also take into account any country specific information that is circulated by the government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations Security Resolutions.
5. 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.
6. The RE shall accept the clients based on the risk they are likely to pose. For this purpose, the RE shall categorize the clients under low risk, medium risk and high-risk category as follows:
 - a) **Low Risk:** Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. The illustrative examples of low-risk clients are:
 - Salaried employees whose salary structures are well defined
 - Businessman whose identity and source of wealth is easily identified and who is complying with maximum KYC disclosures.
 - People belonging to lower economic strata of the society whose accounts show small balances and low turnover
 - Government Departments and Government owned companies
 - Regulators and statutory bodies etc.
 In such cases, only the basic requirements of verifying the identity and location of the customer shall be met.
 - b) **Medium Risk:** Clients that are likely to pose a higher than average risk to the RE may 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; such as:

- Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
 - Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious
 - Clients delegating authority of operation of their trading & beneficial accounts to any of their immediate family members.
 - Corporate which are providing financial details of last two years and identity of the beneficial owner is disclosed.
 - HNI's who have respectable social and financial payments, etc.
- c) **High Risk:** The staff may apply enhanced 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. The examples of customers requiring higher due diligence may include:
- High net worth individuals whose identity and source of wealth could not be established
 - Trusts, charities, NGOs and organizations receiving donations
 - Politically Exposed Persons (PEPs) of foreign origin
 - Non-face to face customers
 - Firms with 'sleeping partners'
 - Companies having close family shareholding or having multi-layer corporate structure whose beneficial ownership could not be identified/ established
 - Those with dubious reputation as per public information available
 - Clients in high risk countries as announced by appropriate authority from time to time
 - Non-Resident clients whose identity could not be established
- d) The RE shall categorize the following clients as "Clients of Special Category (CSC)":
- Non - resident clients
 - High net-worth clients
 - Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
 - Companies having close family shareholdings or beneficial ownership
 - Politically Exposed Persons (PEPs). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. The additional norms applicable to PEP as contained in the subsequent paragraph of Client Identification procedure of this policy shall also be applied to the accounts of the family members or close relatives / associates of PEPs
 - Clients in high risk countries. While dealing with clients from or situated in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places

where existence or effectiveness of action against money laundering or terror financing is suspect, intermediaries apart from being guided by the Financial Action task Force (FATF) statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to.

- The intermediary shall specifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
- Non face to face clients
- Clients with dubious reputation as per public information available etc.

The RE shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

V. Monitoring of transactions

1. Ongoing monitoring is an essential element of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account.
2. The staff shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Transactions that are inconsistent with the size of the balance maintained may indicate that the funds are being 'washed' through the account. High risk accounts shall be subjected to intensive monitoring. 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 are required to be maintained and preserved for a period of five years from the date of transaction between the client and the RE
3. The staff shall apply client due diligence measures to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.
4. The RE shall preserve and maintain a record of the transactions in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act shall be reported to the Director, FIU-IND.
5. The Compliance Department shall ensure adherence to the KYC policies and procedures. It 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.

7.0 Suspicious transaction monitoring and reporting

1. The information on Financial Status/income details of clients should be obtained at the time of opening of client account. Subsequently, Financial Status/income details of clients should be periodically updated in the records of the RE and the regulatory authorities, etc. The RE shall identify cases where volume of client's transaction is not commensurate with the known source of income/ net worth of the customer. If any abnormality is noticed, the RE should file STR with FIU-IND
2. No transaction or account-based relationship shall be undertaken without following the CDD procedure.
3. The RE shall update the financial details of customer on periodical basis.
4. Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses if any observed in this regard. The compliance in this regard shall be put up before the management on half yearly intervals. All staff members shall be provided training on Anti Money Laundering. The focus of training shall be different for frontline staff, compliance staff and staff dealing with new customers.
5. Suspicious transactions shall also be regularly reported to the higher authorities within the RE.
6. Employees, officers and Directors shall ensure strict confidentiality of the STR filed with FIU and shall not be disclosed/ communicated/ tipped off to the customer or any other person.

7. Monitoring Process

The Principal Officer shall ensure continuous monitoring of the transactions of the Customers to identify suspicious transactions. Following transactions / activities may be identified as Suspicious transactions as notified by SEBI/ FIU-IND:

- 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 in high-risk jurisdictions or clients introduced by banks or affiliates or other 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 shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items
- h) Cheque towards the investment is issued by payer other than the account holder and the account holder refuses to give declaration that the source of fund is legitimate.
- i) Investor induces towards non filing of returns or forms to regulatory bodies.

- j) Unusual request is made from the client like not to send account statements
- k) Sudden increase \ decrease in the number of transactions by the client.
- l) Inoperative accounts suddenly becoming operative/ highly active.
- m) There are frequent changes in the address of client.
- n) Documents sent to the client are returned undelivered frequently.
- o) Off Market Transactions insisted by the client.
- p) Volume of transactions does not commensurate with the known source of income/ networth of the customer.

The above list can be modified to add any other type of transactions/activities as and when required.

8. The RE may, if required, implement further enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence in case of 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, categorized as 'CSC'.

8.0 Information to be maintained

The RE shall maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

- i. The nature of the transactions
- ii. The amount of the transaction and the currency in which it is denominated
- iii. The date on which the transaction was conducted and
- iv. The parties to the transaction.

9.0 Record Keeping

- i. The RE shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.
- ii. 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 shall be maintained.
- iii. Shall 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, registered intermediaries shall retain the following information for the accounts of their clients 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.
- iv. The RE shall ensure all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.
- v. A system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules as mentioned below are put in place:
- a) All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency
 - b) 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
 - c) 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
 - d) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- vi. Where the RE does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the registered intermediary shall close the account of the clients after giving due notice to the client.
- Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under rules 3 and 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

10.0 Retention of Records

- The RE shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities.
- The records mentioned in Rule 3 of PML Rules shall be maintained and preserved for a period of five years from the date of transactions between the client and intermediary.
- The records evidencing the identity of clients are maintained and preserved for a period of five years from the date of cessation of transactions between the client and intermediary, i.e. the date of termination of an account or business relationship between the client and intermediary.
- The following document retention terms shall be observed:

- i. All necessary records on transactions, both domestic and international, are maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA and rules framed thereunder as well SEBI Act) and other legislations, Regulations or exchange bye-laws or circulars.
 - ii. The RE shall maintain and preserve the records of documents evidencing the identity of its 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 intermediary has ended or the account has been closed, whichever is later.
- In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they are retained until it is confirmed that the case has been closed.
 - **Records of information reported to the Director, Financial Intelligence Unit - India (FIU - IND):** The RE shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU - IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the intermediary.

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

- The RE shall ensure that it does not have any accounts in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC)
- The RE shall ensure strict compliance with Government of India issued order on procedure for implementation of section 51A of the Unlawful Activities (Prevention) Act, 1967 and amendments/corrigendum issued thereon.

12.0 Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 - Directions to stock exchanges and registered intermediaries

- The RE shall ensure compliance with Government of India issued order on "Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act") and amendments thereon.
- The RE shall maintain list of individuals/entities ("Designated List") and update it, without delay, in terms of paragraph 2.1 of the Order
- The RE shall verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, stock exchanges and registered intermediaries shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), without delay. The details of the CNO are as under: The Director, FIU-INDIA, Tel.No.:011-23314458, 011-23314459 (FAX), Email: dir@fiuindia.gov.in

- The RE shall run a check, on the given parameters, at the time of establishing a relation with a client and on a periodic basis to verify whether individuals and entities in the Designated List are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, insurance policies etc. In case, the clients' particulars match with the particulars of Designated List, stock exchanges and registered intermediaries shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books to the CNO, without delay
- The RE shall send a copy of the communication, mentioned in paragraphs 59(ii) and 59(iii) above, without delay, to the Nodal Officer of SEBI. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the Nodal Officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051
- The RE shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, in case there are reasons to believe beyond doubt that funds or assets held by a client would fall under the purview of Section 12A (2)(a) or Section 12A(2)(b) of the WMD Act
- The RE shall file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered under paragraphs 59(ii) and (iii) above, carried through or attempted through.
- Upon the receipt of the information above, the CNO would cause a verification to be conducted by the appropriate authorities to ensure that the individuals/entities identified are the ones in the Designated List and the funds, financial assets or economic resources or related services, reported are in respect of the designated individuals/entities. In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under section 12A would be issued by the CNO and be conveyed to the RE so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/entities.
- The RE shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

13.0 **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> and the same is updated from time to time.
- The RE shall ensure that accounts are not opened in the name of anyone whose name appears in said list.
- The RE 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.

- The RE shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.
- The RE shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.
- The RE shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affair.

14.0 Jurisdictions that do not or insufficiently apply the FATF Recommendations

- FATF Secretariat after conclusion of each of its plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by the registered intermediaries.
- The RE shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the regulated entities are not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

15.0 Reporting to Financial Intelligence Unit-India (FIU IND)

- i. The RE shall initially register on the portal of FIU-IND and create its login id on <https://finnet.gov.in>.
- ii. Any suspicious transactions need to be notified immediately to the Principal Officer. The notification may be done in the form of a detailed report with specific reference to the client's transactions and the nature or reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told other wise and the client should not be told of the report or suspicion.

series of transactions integrally connected are of suspicious nature. The Principal Officer shall on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 of the PML Rules. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion

- d) The Non Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month
- e) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
- f) Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
- g) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.
- h) Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)
- i) The RE shall not put any restrictions on operations in the accounts where an STR has been made. The RE 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
- j) Every registered intermediary, its Directors, officers and all employees shall ensure that the fact of maintenance referred to in Rule 3 of PML Rules and furnishing of information to the Director is kept confidential.
- k) Provided that nothing in this rule shall inhibit sharing of information under Rule 3A of PML Rules of any analysis of transactions and activities which appear unusual, if any such analysis has been done
- l) The RE shall irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in this policy shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.
- Confidentiality requirement does not inhibit information sharing among entities in the group

16.0 Designation of officers for ensuring compliance with provisions of PMLA

I. Appointment of a Principal Officer

To ensure that the registered intermediaries properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would 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-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by a registered intermediary; Provided that such officer shall be an officer at the management level

II. Appointment of a Designated Director

The RE shall also designate a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under: "Designated director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes –

- a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,
- b) the managing partner if the reporting entity is a partnership firm,
- c) the proprietor if the reporting entity is a proprietorship firm,
- d) the managing trustee if the reporting entity is a trust,
- e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
- f) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above."

The RE is aware that 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 RE shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

17.0 AML Team

An AML team is formed, as under, which monitors the transactions listed above on an ongoing basis, analyses transactions, identifies transactions that are suspicious in nature and reports the same to the concerned authority through the Principal Officer.

Composition of AML Team:

Designated Director
Principal officer

18.0 Hiring of Employees and their Training

- i. The staff required for the RE is appointed by the RE after proper screening. The RE shall follow standard procedures for hiring employees.
- ii. Key positions in the RE are identified and it is ensured that the employees taking up these positions are suitable and competent to perform their duties.

- iii. The RE has an ongoing employee training programme to adequately train the members of the staff in AML and CFT procedures. Training requirements has specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. The RE shall ensure that 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.

19.0 Investors Education

Implementation of AML/CFT measures requires the RE 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. The RE shall, therefore, sensitize its clients about these requirements as the ones emanating from AML and CFT framework. The RE shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

20.0 Review of the Policy

The policy will be reviewed periodically and shall be updated as per the directions/ Circulars issued by SEBI and other regulatory authorities from time to time.

Annexure- I: Customer Identification Requirements – Indicative Guidelines

Particulars	Guidelines
Trust/Nominee or Fiduciary Accounts	<p>There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The staff should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, staff shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, staff should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.</p>
Accounts of companies and firms	<p>Staff needs to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the RE. Staff should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.</p>
Client accounts opened by professional intermediaries	<p>When the staff member has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Staff may hold 'pooled' accounts managed by professional intermediaries on behalf of Entities like mutual funds, pension funds or other types of funds. Staff should also maintain 'pooled' accounts managed by lawyers/chartered accountants or stock the RE for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the Intermediaries are not co-mingled at the branch and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such accounts are co-mingled at the branch, the branch should still look through to the beneficial owners. Where the RE rely on the 'customer due</p>