

# **ANTI MONEY LAUNDERING POLICY**

NBSPL - Member BSE , NSE , MCX , NCDEX , MSEI .

SEBI - INZ000202536

**SEBI Master Circular on Anti Money Laundering (AML and Combating Financing of Terrorism (CFT) - Obligations of Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules Framed there-under dated February 03, 2023 and SEBI Circulars issued thereunder from time to time.**

**POLICY CONTROL**

<b>Effective Date</b>	01.10.2025
<b>Frequency of Review</b>	Yearly or as and when any update comes change in the Relevant Regulation comes or any change in the Company's internal control or Structure whichever is earlier.
<b>Next Review Date</b>	30.09.2026

**SEBI Master Circular on Anti Money Laundering (AML and Combating Financing of Terrorism (CFT) Obligations of Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules Framed there-under dated June 06, 2024, and related SEBI Circulars issued thereunder from time to time.**

**I. INTRODUCTION:**

**Nirmal Bang Securities Private Limited** wishes to be at the forefront, towards ensuring compliance with all the regulatory requirements and is committed to maintaining and promoting high ethical standards and business practices. As an effort in the same direction, we have prepared this Anti-Money Laundering Policy & Procedures ("Policy") in order to ensure compliance under the Prevention of Money Laundering Act, 2002 and to establish a common vision of our commitment to safeguard India's common values and international peace and security.

Nirmal Bang Securities Private Limited is an intermediary under the Prevention of Money Laundering Act, 2002; ("PMLA") is required to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to law enforcement authorities. The Policy is intended to establish certain guiding principles for all employees and consultants of Nirmal Bang Securities Private Limited.

**II. BACKGROUND:**

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Necessary Notifications/Rules notified there under came into force with effect from July 1, 2005. Subsequently, SEBI issued necessary guidelines vide circular no. ISD/CIR/RR/AML/1/06 dated 18<sup>th</sup> January 2006 and vide letter No. ISD/CIR/RR/AML/2/06 dated 20<sup>th</sup> March 2006 to all securities market intermediaries as registered under Section 12 of the SEBI Act, 1992. The Maintenance of Records Rules empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and form in which it is to be maintained.

Further, every reporting entity shall have to adhere to the client account opening procedures, maintenance records, and reporting of such transactions as prescribed by the PMLA and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (Maintenance of Records Rules), as amended from time to time and notified by the Government of India. The PMLA inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as provided in Section 12A read with Section 24 of the SEBI Act will be treated as a scheduled offence under schedule B of the PMLA.

The Guidelines mandates that every reporting entity to evolve an internal mechanism having regard to any guidelines issued by regulator for detecting the transactions specified in the Maintenance of Records Rules and for furnishing information thereof, in such form as may be directed by the regulator.

The Guidelines laid down the minimum requirements, and it was emphasized that the intermediaries may, according to their requirements, specify additional

disclosures to be made by clients to address concerns of Money Laundering and suspicious transactions undertaken by clients.

### III. OBJECTIVE:

The objective of this policy is to:

- a) Create awareness and provide clarity on KYC standards and AML measures.
- b) Outline the obligations under PMLA.
- c) Provide a framework for systems and procedures.
- d) To ensure that our systems can prevent criminal elements from using our business for money laundering
- e) To understand the customers and their financial dealings better, which in turn would help the Company to manage the AML risk prudently.
- f) To put in place appropriate controls for detection and reporting suspicious transactions in accordance with applicable laws/ laid down procedures.

### IV. APPLICABILITY:

These policies and procedures apply to all employees of the Company. The procedures have been established to ensure that all employees know the identity of their customers and take appropriate steps to combat money laundering and terrorist financing.

This Policy is applicable for all segments including Cash, Equity Derivatives, Currency Derivatives, Interest rate Derivatives, Commodities, SLBM and all other segments including in relation to all the Exchanges related to NBSPL. It is also applicable for Depositories of Member NSDL and CDSL.

Adherence to the Policy is a fundamental condition of service with the Company and the provisions of the Policy shall be deemed an intrinsic part of the terms of employment of the Employees. If any Employee experiences any difficulties or doubts in respect of the meaning or interpretation of any of the provisions of the Policy or is unsure of whether a given action would be consistent with the Policy or any other applicable laws, he or she should contact the Designated Director/Compliance Officer (appointed as specified below) for clarifications.

### V. PRINCIPAL OFFICER AND DESIGNATED DIRECTOR:

**Mr. Rakesh Bhandari, Director is appointed as the Principal Officer w.e.f, 1st December, 2019** of the Company.

The Principal Officer shall be responsible to ensure that for compliance with the provisions of the PMLA and AML Guidelines, overseeing the implementation of this Policy, acting as a central reference point, and reporting if any on the issues covered herein to the Board of Directors. Further, the Principal officer is to play an active role in the identification & assessment of potentially suspicious transactions. Employees

shall refer all matters concerning the issues covered by this Policy to the Designated Principal Officer and shall act in accordance with his/her instructions on this behalf.

The Principal Officer will keep the Designated Director and the Board of Directors informed about the issues if any covered by the Policy. In the absence of the Principal Officer, the Chief Executive Officer/Managing Director shall discharge the obligations of the Principal Officer under this Policy. The principal officer shall be responsible for maintaining and updating all records to be kept in accordance with this Policy or any applicable laws/regulations.

### **Rights & Power of Principal Officer**

- Overall monitoring & implementation of the company's KYC/AML/CFT policy and to make changes/amendments in the PMLA/CFT policy of NBSPL time to time along with requirement of Record Keeping, retention, monitoring and reporting.
- To ask details related to ultimate beneficiary ownership/person controls securities account/POA Holder /Nominee in case it seems to be suspicious.
- To ask specific nature of its business organizational structure, income details and its way and about the nature of transaction etc., of its clients and its business related entities.
- To verify the customer identity and to refuse in opening any trading/DP account if client acceptance policy has not been met or Client has not fulfilled his due diligence measures, including requirements for proper identification and in-person verification or in case where client account has been opened in Benami name. The same refusal can be applied also based on clients' location (permanent address, registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions.
- Conduct of 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. Special checks and permission for clients of special category (CSC) and transaction related to foreign exchange transaction related entities.
- Verification and denial in taking the person as a client if the person is in 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) from the website.
- To 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 NBSPL's knowledge of the client, its business and risk profile and the client's source of funds.

- Stopping of the business of Intermediary in case of manipulation at its end or in providing any support to client who is engaged in any kind of manipulative trading. To approve or disapprove the mode of payment opted by the client, especially in case of Cash, Demand draft, Pay order or any other mode which seems to be suspicious or crossing any regulatory limits defined.
- Immediately stopping of Pay-in or Pay-out of funds/Securities or both if by any means the suspicious Trading pattern /wrong account information or other details has been observed.
- Monitoring, investigation and taking action against all suspicious transactions (transactions integrally connected', 'transactions remotely connected or related) whether made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat account, security account maintained by NBSPL.
- In handling and reporting of transactions {Cash Transaction Reports (CTRs), Suspicious Transaction Reports (STRs), Non - Profit Organization Transaction Report (NTRs) and Counterfeit Currency Reports (CCRs)} and sharing of information/details, as required under the law in an independent manner and Co-operation with the relevant law enforcement authorities, including the timely disclosure of information. In addition to this the maintenance of utmost confidentiality in filing of CTR, STR and NTR to FIU-IND.
- Dealing with regulators like SEBI, FIU-INDIA or any other law enforcement agency including ministries which are involved in the fight against money laundering and combating financing of terrorism.
- In defining the role of Internal audit/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 including 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, 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.
- In conduct of any Program/Seminar/Presentation etc. for the training of the Staff, Registered Intermediary with NBSPL and any other person in connection to the NBSPL to increase awareness and vigilance to guard against money laundering and terrorist financing.

Further, **Mr. Samir Pranal Kamdar, Vice President Compliance is appointed as the Designated Director.** The Designated Director is responsible for ensuring overall compliance by the Company of the obligations imposed under Chapter IV of the PMLA Act and the Rules made thereunder.

## VI. WHAT IS MONEY LAUNDERING?

Money Laundering may be defined as the cleansing of dirty money obtained from legitimate or illegitimate activities including drug trafficking, terrorism, organized crime, fraud, and many other crimes with the objective of hiding its source and rendering it legally usable form. It is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. The process of money laundering involves creating a web of financial transactions to hide the origin and true nature of these funds.

This is done in three phases - **the Placement Phase, Layering Phase & Integration Phase.**

- i. **Placement Phase** - The placement stage involves the physical movement of currency or other funds derived from illegal activities to a place or into a form that is less suspicious to law enforcement authorities and more convenient to the criminal. The proceeds are introduced into traditional or non-traditional financial institutions or the retail economy.
- ii. **Layering** - The layering stage involves the separation of proceeds from their illegal source by using multiple complex financial transactions (e.g., wire transfers, monetary instruments) to obscure the audit trail and hide the proceeds.
- iii. **Integration Phase** - During the integration stage, illegal proceeds are converted into apparently legitimate business earnings through normal financial or commercial operations. Having identified these stages of the money laundering process, financial institutions are required to adopt procedures to guard against and report suspicious transactions that occur at any stage.

## VII. ANTI-MONEY LAUNDERING (AML)PROGRAM:

The objective of having an AML Program is to have adequate policies, practices, and procedures in place to help prevent money laundering. Such practices would include the following:

- ⇒ Appointment of Principal Officer and Designated Director
- ⇒ Adoption of written procedures setting out the process of Client Due Diligence (CDD) comprising of
  - Policy for Acceptance of Clients;
  - Client Identification Procedure;
  - Risk Management;
  - Monitoring of Transactions.
- ⇒ Recordkeeping & retention of records
- ⇒ Submission of reports to Finance Intelligence Unit- India (FIU-IND) in the prescribed formats of CTR, STR, and NTR as and when such reporting arises

- ⇒ Co-operating with law enforcement agencies including the timely disclosures of information.
- ⇒ On-going training to the employees to ensure strict adherence to CDD Requirements.

#### VIII. CUSTOMER DUE DILIGENCE PROCESS:

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

- a. Obtain sufficient information to identify persons who beneficially own or control securities accounts. Wherever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person 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. **See Annexure 1 for more details.**
- b. Verify the client's identity using reliable, independent source documents, data and information. 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. 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 as provided with **Annexure -1**
- d. Understanding the ownership and control structure of the client.
- e. Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout 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.
- f. Reviewing 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 suspicious 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; and

- g. To 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..
- h. No transaction or account-based relationship shall be undertaken without following the CDD procedure
- i. To register the details of the client, in case of being a non-profit organization, on the DARPAN Portal of NITI Aayog, and maintain such registration records for a period of five years after the business relationship between a client and the company has ended or the account has been closed, which is later.
- j. If the Company is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, it shall not pursue the CDD process, and shall instead file a STR with FIU-IND.

#### **Consequences of non-furnishing of information**

Where Employees are unable to apply appropriate CDD measure/KYC measures due to the non-furnishing of information and/or in cases where it is not possible to ascertain the identity of the client or the information provided to is suspected to be non-genuine, or there is perceived non-co-operation of the client in providing complete information, such situations should be brought to the notice of the Designated Principal Officer (PO).

The Designated PO may, after consulting with the senior management, consider closing the Client's account or terminating the business relationship and if found necessary, file a suspicious activity report with Financial Intelligence Unit (FIU). The Principal Officer shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account.

The Employees shall be cautious to ensure that the securities or money of the Client that may be linked to the suspicious trades is not returned. However, the Principal Officer shall consult the relevant authorities in determining what action shall be taken in case of such suspicious trading.

#### **IX. CUSTOMER ACCEPTANCE POLICY:**

The Company is committed to ensuring that the guidelines regarding the Customer/business acceptance policy are strictly followed. Existing/past

relationships with the client should be verified and we should ensure that the client is not on the list of Designated Individuals/Entities.

a) **Each client should be met in person:**

To accept new clients, either an Employee must meet the Clients at the Company's offices or visit the residence/office address of the client. As far as possible, it should be ensured that the new client is introduced by an existing client, or it is known to any employee or partner of the Company.

Detailed search to be carried out to find that the Client is not in defaulters /negative list of regulators. (Search may invariably be carried out on SEBI website [www.sebi.gov.in](http://www.sebi.gov.in) and Ministry of Company Affairs, etc.)

An assessment should be made of the financial worthiness of the client by obtaining appropriate declarations at the KYC Stage. This information should be subsequently used to monitor whether transactions of the Client are within the declared means and if the value of the transactions is increasing the client should be asked to disclose sources of increase in their means.

b) **Accepts clients on whom we are able to apply appropriate KYC Procedures:**

Obtain complete information from the client. It should be ensured that the initial forms taken by the client are filled in completely. All photocopies submitted by the client are checked against original documents without any exception. Ensure that the 'Know Your Client' guidelines are followed without any exception.

All supporting documents as specified by the Securities and Exchange Board of India (SEBI) are to be obtained and verified.

c) **Do not accept clients with identity matching persons known to have a criminal background:**

Check whether the client's identity matches with any person having a known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement / regulatory agency worldwide.

Employees should take into account any country-specific information circulated by the Government of India and SEBI from time to time and the updated list of individuals and entities who are subjected to sanctions by United Nations Security Council Regulations (available at <https://www.un.org/securitycouncil/>). Individuals and Entities who have been banned by SEBI from trading in the stock market should not be accepted as Clients.

**d) Be careful while accepting Clients of Special categories:**

We should be careful while accepting clients of special categories like:

a. Non-Resident clients,

b. High net-worth clients,\*

High net worth clients could be classified if at the account opening stage or during the course of the relationship, it is realized that the client's investments or the appetite for investment is high. The High-net-worth clients are basically categorized as the clients having a Net worth of Rs. 10 Crores or more.

c. Trust, Charities, Non-Governmental Organizations (NGOs), and organizations receiving donations,

d. Companies having close family shareholdings or beneficial ownership,

e. Politically Exposed Persons (PEP)

Explanation 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 parts of the Policy shall also be applied to the accounts of the family members or close relatives/associates of PEPs.

Similarly, for Domestic PEPs, they are also considered as high-risk individuals and are located in the same country as of the Company of which it is a client and has a domestically located position. These domestic high-risk individuals are defined as officials of a local political party, senior politicians, heads of state companies, or senior military officials, etc.

f. Clients in high-risk countries where the existence/effectiveness of money laundering controls or terror financing is suspect, countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website ([www.fatf-gafi.org](http://www.fatf-gafi.org)) from time to time. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high-risk countries and geographic areas or delivery of services through such high-risk countries. The company 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.

g. Non-face to face clients

Explanation - Non-face to face clients means clients who open account without visiting the branch/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video Based customer identification process is treated as face-to-face onboarding of the clients.

h. Clients with dubious reputation as per public information available etc.

i. Persons of foreign origin, companies having closed shareholding/ownership, companies dealing in foreign currency, shell companies, overseas entities, clients in high-risk countries.

**\* High Net worth clients means:**

High net worth clients could be classified if at the account opening stage or during the course of the relationship, it is realized that the client's investments or the appetite for investment is high. The High-net-worth clients are basically categorized as the clients having a Net worth of Rs. 10 Crores or more.

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

e) **Do not accept client registration forms that are suspected to be fictitious:**

Ensure that no account is being opened in a fictitious / benami name or on an anonymous basis. The employees shall follow the applicable SEBI guidelines read in conjunction with this policy.

f) **Do not compromise on submission of mandatory information/documents:**

The client's account should be opened only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Do not open the accounts where the client refuses to provide information/documents.

**X. CUSTOMER IDENTIFICATION PROCEDURE:**

In order to prevent the opening of any account which is fictitious/benami/anonymous in nature, the following Customer Identification guidelines should be adhered to:

- a. The Company will register the Clients as per the SEBI Guidelines issued thereunder from time to time and it will develop an appropriate reporting system to monitor clients' accounts.
- b. Special care would be taken in case of non-individual accounts such as corporate, partnership firms, etc., where the ownership structure is opaque. In all such cases, the accounts would be activated only post approval from the compliance department. For this purpose, "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. **(See Annexure 1 for details.)**
- c. The Company shall implement the procedure to determine whether the potential client is a Domestic politically exposed person. It is required to obtain senior

management approval for establishing/ continuing business relationships with PEPs.

- d. Caution is to be exercised when identifying companies that appear to be 'shell companies' or 'front companies. Shell/front companies are legal entities that have no business substance in their own right but through which financial transactions may be conducted.
- e. In case of clients acting through Power of Attorneys the principal and agent should come in person for the first time, except where the client is a NRI and the designated branch of the Authorized Dealer Bank is holding the power of attorney. Photos of both to be obtained along with signatures on the photos. The KYC Form, Member Constituent Agreement and the Risk Disclosure Document must compulsorily be signed by the Client himself and not by the POA holder except in case of NRI clients if the POA holder is the designated branch of the authorized dealer.
- f. Original of un-expired Photo identity of individual/promoter/director to be verified by our official for identifying the client. Signature of the persons should be obtained on the photos. Photocopy of the proof should be taken by our official who should also certify thereon about having verified with the unexpired original.
- g. Special care would be taken in the case of non-individual accounts such as corporate, partnership firms, etc., where the ownership structure is opaque. In all such cases, the accounts would be activated only post approval from the compliance department. For this purpose, "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. (See Annexure 1 for details.)
- h. Verify originals of the KYC/ ID documents of the client. **See Annexure 2 for a list of documents that can be obtained/ relied upon to complete KYC checks.**

The Company may modify the Account Opening Form to obtain the necessary information of the client to achieve, whenever necessary PMLA objective.

If the applicant has completed KYC Procedure with the Central KYC Records Registry (CKYCR) or any KYC Registration Agency (KRA) as applicable, in-person verification will not be required.

Company may also conduct online KYC Comprising KYC through online/App, in-person verification through video, online submission of an Officially valid document or other documents under e-sign while onboarding new clients by following the procedures laid down by SEBI and advised by KYC Registration Agencies from time to time.

The Company if, opting to conduct online KYC through safe and secured technological innovations should adhere to circular no.

SEBI/HO/MIRSD/DOP/CIR/P/202 dated 24<sup>th</sup> April 2020 or such other circulars as issued by SEBI.

**The company may rely on a third party for the purpose of:**

1. Identification and verification of the identity of a client and
2. 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 a 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.
3. 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 regulation and circulars / Guidelines issued by SEBI from time to time. Further, it is clarified that Member shall be ultimately responsible for CDD and undertaking enhanced due diligence measures as applicable. (SEBI Circular CIR/MISRD/1/2014 dated 12.03.2014)

**XI. RISK MANAGEMENT:**

The Company has a Risk Based Approach (RBA) for mitigation and management of the identified risk and also have a risk management policy in regard to the identification of the risk, controls and procedures approved by the senior management.

Risk assessment on money laundering is dependent on the 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.

The Risk Assessment is required

- to assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.
- to 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 Company shall ensure:

- a. To undertake the ML/TF risk assessments prior to launch or use of such products, practices, services, technologies; and
- b. Adoption of a risk-based approach to manage and mitigate the risk.
- c. Take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

Clients will be categorized based on the risk parameters set out below and classified as - low risk, medium risk, and high risk. No client will be exempted from KYC procedures.

**(i) High Risk**

In addition to client defined in special category, clients who have defaulted in the past, have suspicious background, do not have any financial status and following clients are classified as high risk, provided their transaction value exceeds Rs. 1 million (I.e, Rs. 10 Crores).

a. Non-Resident clients,

b. High net-worth clients,\*

High net worth clients could be classified if at the account opening stage or during the course of the relationship, it is realized that the client's investments or the appetite for investment is high. The High-net-worth clients are basically categorized as the clients having a Net worth of Rs. 10 Crores or more.

c. Trust, Charities, Non-Governmental Organizations (NGOs), and organizations receiving donations,

d. Companies having close family shareholdings or beneficial ownership,

e. Politically Exposed Persons (PEP)

Explanation - 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 parts of the Policy shall also be applied to the accounts of the family members or close relatives of PEPs.

Similarly, for Domestic PEPs, they are also considered as high-risk individuals and are located in the same country as of the Company of which it is a client and has a domestically located position. These domestic high-risk individuals are defined as officials of a local political party, senior politicians, heads of state companies, or senior military officials, etc.

f. Clients in high-risk countries where the existence/effectiveness of money laundering controls or terror financing is suspect, countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website ([www.fatf-gafi.org](http://www.fatf-gafi.org)) from time to time. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries.

g. Non-face to face clients

Explanation - Non-face to face clients means clients who open account without visiting the branch/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video Based customer identification process is treated as face-to-face onboarding of the clients.

- h. Clients with dubious reputation as per public information available etc.
- i. Persons of foreign origin, companies having closed shareholding/ownership, companies dealing in foreign currency, shell companies, overseas entities, clients in high-risk countries.

It should be to determine whether existing/potential customer is PEP. Such procedures would include seeking additional information from clients. Further approval of senior management is required for establishment business relationships with PEP & to continue the business relationship with PEP.

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

**(ii) Medium Risk**

Client defined in above category having transaction value below 1 million and those Clients who are mostly intra-day Clients or speculative Clients.

Further based on business directive the clients who maintain running account continuously with the company may also be categorized as Medium risk clients as case to case basis.

**(iii) Low Risk**

Clients those pose Nil or low risk. They are Individuals/Corporate/HNIs who have respectable social and financial standing. These are the Clients who make a payment on time and take delivery of shares. Senior Citizens, Salaried Employees and a major portion of client who indulge in delivery- based trading.

The low risk provisions should not apply when there are suspicions of Money Laundering / Financing Terrorism (ML/FT) or when other factors give rise to a belief that the customer does not in fact pose a low risk.

Apart from this we need to exercise extra caution while monitoring the transactions of NRI/NRE/PIO and foreign clients, especially when the payment is being made in foreign currency.

Any change in the risk profile of the client/mandate holder, has to be ascertained by the concerned branch officials, and reported to the Business Head immediately.

An assessment should be made of the financial worthiness of the client by obtaining appropriate declarations at KYC stage. This information should be subsequently used for monitoring whether the transactions of the clients are within the declared means and if the value of the transactions is increasing the client should be asked to disclose the increasing sources.

The Company shall obtain documents, information for each category of client and apply anti-money laundering measures keeping in view the risk involved in a transaction and performing enhanced due diligence for medium and high-risk clients.

**Risk parameters**

The following factors shall be considered while assessing risk or monitoring suspicious transactions:

- a) Country of residence / registered office of the Client;
- b) nature of business
- c) trading turnover;
- d) manner of making payments for transactions; and
- e) Clients with a dubious reputation or a criminal or political record as per public information available

**Ongoing due diligence:**

The Company will periodically undertake due diligence of its clients to ensure that their transactions are consistent with its knowledge about the client, client's business, risk profile, and source of funds. Where necessary, enhanced due diligence measures will be implemented if the categorization of a client changes from low to medium or high risk.

**Periodic updation:**

Periodic updation of KYC documents shall be carried out in compliance with applicable law.

**XII. MONITORING OF TRANSACTIONS:**

- a) The Company will regularly monitor the transactions to identify any deviation in transactions/activity for ensuring the effectiveness of the AML procedures.
- b) Special attention will be paid to all unusually large transactions/patterns which appear to have no economic purpose.
- c) The Company will from time to time specify internal threshold limits for each class of client accounts and pay special attention to transactions that exceed these limits.
- d) The background including all documents/office records /memorandums/clarifications sought to pertain to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records, and related documents shall be made available to auditors and also to SEBI/stock exchanges/FIU-IND/other relevant Authorities, during an audit, inspection, or as and when required.

### **XIII. SUSPICIOUS TRANSACTIONS:**

Employees must report Suspicious transactions whether or not made in cash, to the Designated Principal Officer and/or Compliance officer immediately. Such reports must be submitted in a confidential manner, but the Employee must maintain continuity in dealing with the client as normal until told otherwise. In exceptional circumstances, the Company may discontinue its relationship with a client or take such other action as is considered appropriate. All suspicious transactions will be reported to the FIU as per applicable law.

#### **What is a Suspicious Transaction?**

Suspicious transaction means a transaction whether or not made in cash, which to a person acting in good faith gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or appears to be made in circumstance of unusual or unjustified complexity or appears to have no economic rationale or bonafide purpose or gives rise to a reasonable ground of suspicious that it may involve financing activities relating to terrorism.

#### **Reasons for Suspicious:**

##### **Identity of client**

- False identification documents
- Identification documents that could not be verified within a reasonable time
- Non-face to face client
- Clients in a high-risk jurisdiction
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities
- Receipt back of welcome kit undelivered at the address given by the client
- Suspicious background or links with criminals

##### **Suspicious Background**

- Suspicious background or links with criminals

##### **Multiple Accounts**

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

##### **Activity in Accounts**

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

- Account used for circular trading

#### **Nature of Transactions**

- No economic rationale or bonafide purpose
- The Source of funds is doubtful
- Appears to be case of insider trading
- Purchases made on own account transferred to a third party through an off market transactions through DP account
- Transactions reflect likely market manipulation
- Suspicious off market transactions

#### **Value of Transactions**

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

#### **Identifying and Reporting suspicious transactions:**

The Principal Officer for any suspicious transactions will scrutinize transactions filtered out of the following filters in detail. As the Business dynamics are very varied and complex, defining transaction types for reporting will not be undertaken at this juncture (all CTRs, STRs and NTRs). Having said that, the Principal Officer will review all the transactions thrown out by the filters and decide on a case-to-case basis to report to FIU within stipulated time with complete details.

Further, no nil reporting shall be made if there is no Cash / Suspicious / Non - Profit organization transactions.

These filters will be reviewed regularly for any updations and modifications to make the system more robust and effective.

1. Payment for Payout to all the clients will be only through cheque. No cash payments to be entertained under any circumstances.
2. All third party cheques to the credit of clients account irrespective of the amount.
3. All payment made either by way of Demand Draft / Cheques / Money Transfer/Funds Transfer in foreign currencies irrespective of the amount. In case of DD it should be accompanied by the letter of bank in case of some unavoidable situation.
4. Deliveries/Payment made through us for more than 250% of the last 3 months average.

5. To discourage the manipulation relating to the financial strength, we have started the provision of updating the financial statements of the clients annually and this is the ongoing procedure.

**What to Report:**

- The nature of the transactions
- The amount of the transaction and the currency in which it was denominated
- The date on which the transaction was conducted
- The parties to the transaction.
- The reason of suspicion.

There shall not be any restrictions on operations in the accounts where an STR or NTR has been made. Member and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing (“tipping off”) the fact that a STR or NTR 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/ NTR and/or related information but even before, during and after the submission of an STR/NTR. Thus, it shall be ensured that there is no tipping off to the client at any level.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, member shall file STR/NTR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

**Suspicious transactions Reporting:**

The Staff of the Operations department concerned shall monitor all transactions executed by the clients and report the same to the HOD and in turn to the “Principal Officer” for any transactions that appear to be of suspicious nature. They shall hand over a detailed report to the Principal Officer comprising details such as clients and transaction details and the nature or reason for suspicious.

In case the principal officer finds the transactions to be of suspicious nature, then it shall submit the report of such transactions to the Director, FIU-INDIA in the prescribed format, promptly on the establishment of suspicion. In case transactions are abandoned or aborted by clients, on being asked to give some details or to provide the document, the company shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

The Directors, Officers and all the Employees will ensure complete confidentiality in regards to the furnishing of the information to the Director and maintenance of the records as mentioned in Rule 3 of the PMLA Rules, 2005.

The Company shall adhere to the following while reporting transactions to FIU-IND:

1. The Cash Transaction Report (CTR) (whenever applicable) for each month shall be submitted to FIU-IND by the 15<sup>th</sup> of the succeeding month;
2. 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 is of suspicious nature. 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;
3. The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by the 15<sup>th</sup> of the succeeding month; Explanation - Non-profit Organization means any entity or organization, 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, 1980 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);
4. The Principal Officer will be responsible for timely submission of CTR, STR, and NTR to FIU-IND;
5. Utmost confidentiality shall be maintained in the filing of CTR, STR, and NTR to FIU-IND; and
6. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious/non-profit organization transactions to be reported.

#### **XIV. RECORD KEEPING:**

The Company shall comply with the record-keeping and 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.

The Company shall maintain a proper record of the nature and the value of all transactions which has been prescribed under Rule 3 of the PML Rules as below:

- a. All cash transactions of the value of more than Rs 10 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 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month and the monthly aggregate exceeds an amount of Rs. 10 lakhs or its equivalent in foreign currency.  
It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.
- c. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.

- d. 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.

Where the company does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which it 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

All records evidencing identity of clients and beneficial owners, all KYC-related documents, transaction-related information, account files, and business correspondence shall be maintained and preserved for 5 (five) years after the business relationship with the client has ended or the account has been closed, whichever is later.

As required and as stated in SEBI (Depositories and Participants) Regulations, 2018 and circulars issued thereunder, the records as required under Depositories shall be maintained for a minimum period of eight (8) years.

The information which needs to be maintained includes:

- a) Nature of transactions
- b) Amount of transaction and currency in which it was denominated
- c) Date on which transaction was conducted
- d) Parties to the transaction
- e) Information pertaining to cash transactions of more than Rs. 10 lakhs (or its equivalent in foreign currency), all series of cash transactions integrally connected to each other which might have been individually valued at less than Rs. 10 lakhs but aggregate to more than Rs. 10 lakhs, all suspicious transactions (whether or not made in cash).

All documents & records which 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 the prosecution of criminal behavior shall be maintained and retained in accordance with applicable law including the PML Rules.

All information reported to regulatory authorities/ investigating agencies including FIU shall be maintained and preserved for 5 years from the date on which the Company ceases to transact with the client or up to the end of investigation/ inquiry

by FIU/ regulatory/ investigating agencies (where the Company has been intimated about any investigation), whichever is later.

#### **Audit trail**

To enable the reconstruction of information or financial profile of any suspect account or of any suspect laundered money or terrorist property for purposes specified under the Act, the company shall retain the following information in order to maintain a satisfactory audit trail:

- The beneficial owner of the account
- The volume of the funds flowing through the account / and for the selected transactions
  - The origin of the funds
  - The form in which the funds were offered or withdrawn, e.g. cheques, bank drafts/pay orders, etc.
  - The identity of the person undertaking the transaction
  - The destination of the funds
  - The form of instruction and authority
  - The identity of the official who conducted in-person verification, and who verified copies of documents obtained from the client with originals.

The aforesaid information shall be retained for a minimum period of 5 years and the said retention period shall be modified on receiving appropriate instructions from any regulatory like SEBI, FIU IND, or any other statutory authority.

#### **XV. 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 29, 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, 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 obligations to be followed by intermediaries to ensure the effective and expeditious implementation of said Order have been issued vide SEBI Circular ref. no.

ISD/AML/CIR-2/2009 dated October 23, 2009, which needs to be complied with scrupulously.

The Company shall ensure that in terms of Section 51A, they do not have any accounts in the name of the individuals/entities appearing in the list of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council. (UNSC).

Accordingly, SEBI has issued circular ref.no SEBI/HO/MIRSD/DOP/CIR/P/2021/36 dated March 25, 2021, which outlines a revised and effective implementation of the provisions of Section 51A through an order dated February 02, 2021, superseding the earlier orders and guidelines given on the said subject for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021. A corrigendum dated March 15, 2023 has also been issued in this regard. This List of Nodal Officers for UAPA is available on the website of MHA.

**Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act):**

The Company shall comply with the Government of India, Ministry of Finance Order dated **January 30, 2023** (F. No. P-12011/14/2022-ES Cell-DOR) issued for implementation of **Section 12A of the WMD Act**. Accordingly, the Company shall

- a) **maintain and update, without delay, the list of individuals/entities (Designated List)** as prescribed in the said Order;
- b) **verify** whether any client / beneficial owner / counterparty to a financial transaction matches the Designated List at the time of onboarding and **periodically thereafter**;
- c) where a match is found, the Company shall **not carry out the transaction**, shall **immediately report the transaction details and full particulars of funds/financial assets/economic resources/related services** to the **Central Nodal Officer (CNO)** i.e., Director, FIU-IND (Email: [dir@fiuindia.gov.in](mailto:dir@fiuindia.gov.in)) **without delay**;
- d) the Company shall also **intimate SEBI's Nodal Officer** by sending a copy of such communication **without delay** to [sebi\\_uapa@sebi.gov.in](mailto:sebi_uapa@sebi.gov.in);
- e) the Company shall **prevent the individual/entity from conducting financial transactions** (with intimation to the CNO) where there are reasons to believe beyond doubt that the funds/assets fall under Section 12A(2)(a) or 12A(2)(b) of the WMD Act; and
- f) the Company shall **file a Suspicious Transaction Report (STR)** with FIU-IND covering all transactions carried through or attempted in such accounts.

The Company shall also comply with directions/orders issued by the CNO,

including provisions relating to **exemptions** and **inadvertent freezing**, wherever applicable

**XVI. LIST OF DESIGNATED INDIVIDUALS/ ENTITIES:**

The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. The company shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

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 <https://press.un.org/en/content/press-release>.

The details of the lists are as under:

- a. The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: <https://www.un.org/securitycouncil/sanctions/1267/press-releases>.
- b. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea [www.un.org/securitycouncil/sanctions/1718/press-releases](http://www.un.org/securitycouncil/sanctions/1718/press-releases).

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.

The Company shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

The Company shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

The Company 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.

Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: [jsctcr-mha@gov.in](mailto:jsctcr-mha@gov.in). The Company 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](mailto: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 Affairs.

**XVII. 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 Company 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 company are not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

**XVIII. FINANCIAL INTELLIGENCE UNIT (FIU) - INDIA:**

The government of India set up a Financial Intelligence Unit (FIU-INDIA) on November 18, 2004, as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the finance minister. FIU-INDIA has been established as the central national agency responsible for receiving, processing, analyzing, and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for the coordination and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

In terms with the PML Rules, The reporting of the Cash & Suspicious transactions is to be done to the Director, Financial Intelligence Unit India, (FIU-IND) at the following address:

**Director, FIU-IND,**

Financial Intelligence Unit - India  
6<sup>th</sup> Floor, Tower-Jeevan Bharati Building,  
Connaught Place, New Delhi-110001,  
INDIA Telephone: 91-11-23314429,  
23314459

Email id: [helpdesk@fiuindia.gov.in](mailto:helpdesk@fiuindia.gov.in), [ctrcell@fiuindia.gov.in](mailto:ctrcell@fiuindia.gov.in);  
[complaints@fiuindia.gov.in](mailto:complaints@fiuindia.gov.in)

Website: <http://fiuindia.gov.in>

**XIX. POLICY WITH RESPECT TO EMPLOYEES' HIRING/TRAINING & INVESTOR EDUCATION:**

**The hiring of Key Employees:**

Staffs who deal directly with the public are the first point of contact with potential money launderers. Their efforts are therefore vital to the reporting system for such transactions. Staff should keep abreast of the practices to identify suspicious transactions and on the procedure to be adopted when a transaction is deemed to be suspicious. In short, employees must familiar themselves with their customers' normal trading activities and usual market practices in order to recognize anomalous behavior. Suspicions concerning the source of assets or the nature of a transaction may not be ignored. It is the active responsibility of every person at the company to seek to ensure that the firm's facilities are not being misused.

At the time of screening key employees in the Company, the HR personnel should make sure that the key employees must be made aware about the AML/CFT requirement at the time of joining the organization and on such other time as they deem fit to ensure that key employees\* shall perform & discharge their duties efficiently and effectively to combat risk of money laundering, which is considered to be a prominent area/aspect in an industry in which the company operates.

\*Key employees are employees as per the list maintained by HR personnel from time to time.

**Policy on Employees' training:**

The company should have an ongoing employee training program in terms of following

- Circulating information from time to time to the concerned employees pursuant to the PMLA requirement wherein all the employees are made aware about requirement of PMLA viz. procedures to be followed while dealing with potential clients, ongoing due diligence in terms of risk profile, clients' transactions etc.
- Conducting presentations from time to time to create awareness amongst the concerned employees.

**Policy on Investor Education:**

In order to sensitize clients about the need to provide information to the Company, the Company will endeavor to prepare literature/pamphlets to educate clients of the objective of this Policy.

**Surveillance in sync with AML-**

We have a surveillance department that works in tandem with compliance and RMS and normally takes care of all the activities of clients, branches, remisiers, sub-brokers and other concerned persons of the organization who are in access of any kind of information or are in any way related to the firm. We constantly monitor the activity that destroys the fair and orderly movement of the market and/or involve in suspicious transaction.

**XX. REVIEW OF POLICY:**

The aforesaid AML policy is reviewed on yearly basis or as and when any new circulars issued by the SEBI or relative exchanges, within one month of the same with regard to testing its adequacy to meet the compliance requirements. The Principal Officer is the authority to give directions to undertake additions, changes, modifications etc. as directed by SEBI/ FIU-IND.

**Designated Principal Officer**

In case any further information / Clarification are required in this regard, the principal officer may be contacted.

**Mr. Rakesh Bhandari**

301/302, B-2, Marathon Innova, Opp. Peninsula Building, G.K.Marg, Lower Parel  
(W) -Mumbai -400013 T+91-22-6273 8085

[Rakesh.bhandari@nirmalbang.com](mailto:Rakesh.bhandari@nirmalbang.com)

**XXI. CO-OPERATION WITH STATUTORY AUTHORITIES:**

Employees shall provide all requisite co-operation and assistance to the relevant statutory authorities, including the Securities and Exchange Board of India ("SEBI") and shall comply with all lawful instructions that may be issued by such authorities from time to time. In the event of the Employees receiving any summons, requests, notices or demands from SEBI, income-tax or other statutory authorities or being named parties in any legal proceeding, whether in their personal capacity or otherwise, they shall forthwith inform the Principal Officer in writing of the same and furnish all details as may be required by the Principal Officer in this behalf.

**XXII. ACKNOWLEDGMENT:**

Employees are responsible for reading, understanding, and complying with this Policy, including the supplement or any amendments, modifications made to it from time to time. A copy of the Policy will be provided to all the employees of the Company.

**X-X-X-X-X**

**Annexure forming part of KYC policy & Prevention of Money Laundering Policy**  
**ANNEXURE - 1**

Sr. No	Nature of Client	BO Identification Criteria
1	<b>Company</b>	<p>The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.</p> <p>Explanation:</p> <p>i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;</p> <p>ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;</p>
2	<b>Partnership Firm</b>	<p>The beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.</p> <p>Explanation:</p> <p>"Control" shall include the right to control the management or policy decision</p>
3	<b>AN unincorporated association or body of individuals</b>	<p>The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent of the property or capital or profits of such association or body of individuals.</p>
<p align="center">Where no natural person is identified under clauses (1) or (2) or (3) above, the identity of the relevant natural person who holds the position of senior managing official.</p>		
4	<b>For client which is a trust:</b>	<p>the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the</p>

		trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership;
<b>5</b>	<b>Exemption in case of listed companies:</b>  where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.	
<b>6</b>	<b>Applicability for foreign investors:</b>  Intermediaries dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client.	

|

## ANNEXURE - 2

### **Documents which can be relied upon:**

- **PAN Card:** PAN Card is mandatory and is the most reliable document as it is unique to each individual and is valid for the lifetime of the holder and we can independently check its genuineness through IT Websites.
- **Identity Proof:** PAN Card itself can be served as proof of Identity. However, in the case of PAN card carries an old photograph of the holder, which does not match the current facial features of the client, we should take other identity proof in form of a Voter's identity card, Passport, Ration Card, or any Government / PSU / Bank issued photo identity card / Aadhaar Card.
- **Address Proof:** For Valid address proof, we can rely on the Voter's Identity Card, Passport, Bank Statement, Aadhaar Card, Ration Card, and the latest Electricity/telephone bill in the name of the client. The utility bill should be not more than three months old while entering into a relationship with the clients.

### **Documents to be obtained as part of the customer identification procedure for new clients (unexpired Original should be verified):**

#### **A. Proof of Identity (POI):** - List of documents admissible as Proof of Identity:

- Unique Identification Number (UID) (Aadhaar)
- Passport

- Voter ID card
- Driving license.
- PAN card with photograph.
- Identity card/ document with applicant's Photo, issued by any of the following:
- Central/State Government and its Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, Public Financial Institutions, Colleges affiliated to Universities, Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members; and Credit cards/Debit cards issued by Banks

**B. Proof of Address (POA):** - List of documents admissible as Proof of Address:

(\*Documents having an expiry date should be valid on the date of submission.)

- Passport
- Voters Identity Card
- Ration Card
- Registered Lease or Sale Agreement of Residence/ Driving License/ Flat Maintenance bill/ Insurance Copy.
- Utility bills like Telephone Bill (only landline), Electricity bill or Gas bill - Not more than 3 months old.
- Bank Account Statement/Passbook -- Not more than 3 months old.
- Self-declaration by High Court and Supreme Court judges, giving the new address in respect of their own accounts.
- Proof of address issued by any of the following: Bank Managers of Scheduled Commercial Banks/Scheduled Co-operative Bank/Multinational Foreign Banks/Gazetted Officer/Notary public/elected representatives to the Legislative Assembly/Parliament/Documents issued by any Govt. or Statutory Authority.
- Identity card/document with address, issued by any of the following: Central/State Government and its Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, Public Financial Institutions, Colleges affiliated to Universities and Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members.
- For FII/sub-account, Power of Attorney given by FII/sub-account to the Custodians (which are duly notarized and/or apostilled or consularised) that gives the registered address should be taken.
- The proof of address in the name of the spouse may be accepted.

In the case of non-individuals, additional documents to be obtained from non-individuals, over & above the POI & POA, as mentioned below:

Types of entity	Documentary requirements
<b>Corporate</b>	<ul style="list-style-type: none"> <li>• Copy of the balance sheets for the last 2 financial years (to be submitted every year).</li> <li>• Copy of latest shareholding pattern including the list of all those holding control, either directly or indirectly, in the company in terms of SEBI takeover Regulations, duly certified by the company secretary/Whole-time Director/MD (to be submitted every year).</li> <li>• Photograph, POI, POA, PAN, Aadhaar Card and DIN numbers of whole-time directors/two directors in charge of day to day operations.</li> <li>• Photograph, POI, POA, PAN, Aadhaar Card of individual promoters holding control - either directly or indirectly.</li> <li>• Copies of the Memorandum and Articles of Association and certificate of incorporation.</li> <li>• Copy of the Board Resolution for investment in the securities market.</li> <li>• Authorized signatories list with specimen signatures.</li> <li>• Name of the Relevant Persons Holding Senior Management Position</li> <li>• Address proof of Registered Office and the Principal Place of the Business, if it is different</li> </ul>
<b>Partnership firm</b>	<ul style="list-style-type: none"> <li>• Copy of the balance sheets for the last 2 financial years (to be submitted every year).</li> <li>• Certificate of registration (for registered partnership firms only)</li> <li>• Copy of partnership deed.</li> <li>• Authorized signatories list with specimen signatures.</li> <li>• Photograph, POI, POA, PAN, Aadhaar Card of Partners.</li> <li>• Name of the All the Partners of the Partnership Firm.</li> <li>• Address proof of Registered Office and the Principal Place of the Business, if it is different</li> </ul>
<b>Trust</b>	<ul style="list-style-type: none"> <li>• Copy of the balance sheets for the last 2 financial years (to be submitted every year).</li> </ul>

	<ul style="list-style-type: none"> <li>• Certificate of registration (for registered trust only).</li> <li>• Copy of Trust deed.</li> <li>• List of trustees certified by managing trustees/CA.</li> <li>• Photograph, POI, POA, PAN of Trustees.</li> <li>• Names of the beneficiaries, trustees, settlor and protector, if any and authors of the trust</li> <li>• list of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust</li> <li>• Address Proof of the Registered Office of the Trust.</li> <li>• such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf.</li> <li>•</li> </ul>
<b>HUF</b>	<ul style="list-style-type: none"> <li>• PAN of HUF.</li> <li>• Deed of declaration of HUF/ List of coparceners.</li> <li>• Bank pass-book/bank statement in the name of HUF.</li> <li>• Photograph, POI, POA, PAN of Karta.</li> </ul>
<b>Unincorporated Association or a Body of Individuals</b>	<ul style="list-style-type: none"> <li>• Proof of Existence/Constitution document.</li> <li>• Resolution of the managing body &amp; Power of Attorney granted to transact business on its behalf.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Banks/Institutional Investors</b>	<ul style="list-style-type: none"> <li>• Copy of the constitution/registration or annual report/balance sheet for the last 2 financial years.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Foreign Institutional Investors</b>	<ul style="list-style-type: none"> <li>• Copy of SEBI registration certificate.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Army/Government Bodies</b>	<ul style="list-style-type: none"> <li>• Self-certification on letterhead.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Registered Society</b>	<ul style="list-style-type: none"> <li>• Copy of Registration Certificate under Societies Registration Act.</li> <li>• List of Managing Committee members.</li> <li>• Committee resolution for persons authorized to act as authorized signatories with specimen signatures.</li> <li>• A true copy of Society Rules and Bye-Laws certified by</li> </ul>

	the Chairman/Secretary.
--	-------------------------

**C. List of people authorized to attest the documents:**

1. Notary Public, Gazetted Officer, Manager of a Scheduled Commercial/ Co-operative Bank or Multinational Foreign Banks (Name, Designation & Seal should be affixed on the copy).
2. In the case of NRIs, authorized officials of overseas branches of Scheduled Commercial Banks registered in India, Notary Public, Court Magistrate, Judge, Indian Embassy /Consulate General in the country where the client resides are permitted to attest the documents.

**D.** In case of an NRI account - Repatriable / non-repatriable, the following documents are required: For non-residents and foreign nationals, (allowed to trade subject to RBI and FEMA guidelines), copy of passport/PIO Card/OCI Card and overseas address proof is mandatory.

**E.** In the case of a joint account, the above procedure should be carried out for all the persons who hold the joint account.

**F.** Periodical statement i.e. quarterly (of accounts should be sent to the client (and not power of attorney holder) at his address mentioning that if he does not respond within 30 days of the date of receipt of the letter, the contents shall be taken as approved.

