

UPDATED ANTI MONEY LAUNDERING POLICY

Policy prepared/reviewed by:	Principal officer and Compliance officer
Policy approved by:	Board of Directors
Policy approved on:	December 2024

BACKGROUND

The Prevention of Money Laundering Act, 2002 (hereinafter referred to as “PMLA Act” has come into effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, Government of India.

Securities and Exchange Board of India have issued a circular no. ISD / QR / RR / AML / I/ 06 on January 18, 2006 to all intermediaries registered with SEBI u/s 12 of the SEBI Act, 1992 providing guidelines on Anti-money Laundering (AML) Standards. (hereinafter referred as “Guidelines”). SEBI has now issued circular SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated April 04, 2023 and following Circulars shall stand rescinded from the date of issuance of this Circular

1. SEBI/HO/MIRSD/DOP/CIR/P/2019/113 dated October 15, 2019
2. SEBI/HO/MIRSD/DOP/CIR/P/2021/36 dated March 25, 2021
3. SEBI/HO/MIRSD/DOP/CIR/P/2019/69 dated May 28, 2019
4. CIR/MIRSD/1/2014 dated March 12,2014
5. ISD/AML/CIR/1/2010 dated February 12, 2010
6. ISD/AML/CIR-2/2009 dated October 23, 2009

POLICY STATEMENT

VRM Share Broking Private Limited take measures to combat any effort of laundering money earned through drug trafficking, terrorism and any other means of organized and serious crimes by any individual or entity. Towards this, **VRM Share Broking Private Limited** has put in place all such processes and procedures of internal control aimed at preventing and impeding any attempt of money laundering and terrorist financing using the services offered by the **VRM Share Broking Private Limited**. This policy statement would be with an intent to combat Money Laundering and is as follows:

1. We shall be fully committed to establishing appropriate policies and procedures for the prevention of Money Laundering {ML} and Terrorist Financing {TF} and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Thus we shall ensure that the content of these Directives are understood by all staff members;
2. Have a system in place for identifying, monitoring and reporting suspected transactions to the law enforcement authorities; and
3. Communication of policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities/commodities transactions, money and client records etc. whether in branches, franchisee, departments or subsidiaries;
4. Client acceptance policy and client due diligence measures, including requirements for proper identification , adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF
5. Undertake Client Due Diligence measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship and/or transaction
6. Develop staff members’ awareness and vigilance
7. Maintain records;
8. Compliance with relevant statutory and regulatory requirements;

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

CUSTOMER DUE DILIGENCE PROCESS

We shall obtain sufficient information in order to identify persons who beneficially own or control securities/commodity account. Whenever it is apparent that the securities/commodities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. In-order to carry out the due diligence process, we may rely on a third party only 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. Understand the ownership and control structure of the client;
3. For the purposes of identifying beneficial ownership and control, following shall be verified:

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

1. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

1. *more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;*
 2. *more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or*
 3. *more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.*
2. In cases, where there exists doubt for the above, as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

3. Where no natural person is identified under above clauses, identity of the relevant natural person who holds the position of senior managing official.

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

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

Applicability for foreign investors: Registered 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;

4. 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;
5. We shall on best effort basis periodically update all documents, data or information of all clients and beneficial owners collected under the Client Due Diligence process

CLIENT DUE DELLGENCE

1. We shall not accept any clients who are unable to produce satisfactory documents establishing their identity, as required under the checklist enclosed in their Client Registration Form (CFR) and as modified from time to time under the various regulatory directives.
2. Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.
3. No account shall be allowed to be opened in a fictitious / benami name or on an anonymous basis.
4. Non face to face clients i.e. clients who want to accounts without visiting branch/offices of the Authorised Persons or meeting our officials would not be encouraged, unless video based client identification process is carried out;
5. No account shall be allowed of clients with dubious reputation in case of any public information available etc;
6. If the Principal Officer is of the view that the it is not possible to ascertain the identity of the client, information provided to the Company by the client is suspected to be non genuine or there is perceived non cooperation of the client in providing full & complete information, no business shall be continued with such a client and a suspicious activity report filed with the Office of the Director / Designated Authority, FIU – IND.
7. Wherever there is a suspicion that the identity of the client resembles identity of any person having known criminal background or a person banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency, such case should be brought to the notice of the Principal Officer immediately, before opening an account with the Company. We should not continue to do business with such a person and file a suspicious activity report. It should also evaluate whether there is suspicious trading in determining whether to freeze or close the account.

We should be cautious to ensure that it does not return securities/commodities of money that may be from suspicious trades. For the above, we may consult the relevant authorities in determining what action it should take when it suspects suspicious trading.

8. Relationship Manager/ Branch employees/ Authorised Persons are required to maintain continuous familiarity and follow ups, specially where any inconsistencies are noticed in the information provided with respect to any account being opened.

CLIENT ACCEPTANCE AND IDENTIFICATION

1. All such documents as specified in the checklist of the Client Registration Form as updated from time to time under various regulatory directives for respective categories of clients must be received from the Client at the time of opening of account.
2. If the documentation produced by the prospective client is not in conformity with the requirements specified from time to time or if there are any inconsistencies noticed therein, no account shall be opened and matter to be reported to the Principal Officer immediately.
3. Verify the client's identity using reliable, independent source documents, data or information;
4. 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;
5. 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 above; and
6. As far as possible using reasonable measures, employee dealing with Client should ensure that the person opening the account himself is the beneficial owner or there exists sufficient documentation to corroborate his transacting on behalf of the other person, in which case appropriate due diligence would be done on the beneficial owner as well.
7. Necessary checks and balance are 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. The list which is not limited to has been enumerated :
 - a. SEBI debarred entity list as updated by SEBI/Exchanges
 - b. SEBI /Exchanges/CDSL about 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>
 - c. SEBI /Exchanges/CDSL updates about FATF list
 - d. Identification of Beneficial Ownership of the non-individual clients
 - e. Watchout list
8. 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 registered intermediaries shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.
9. 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.

10. We shall on best effort basis with the available information, documents assess to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. In such cases we shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of Politically Exposed Persons (PEPS) As part of enhanced CDD measures we need to ensure senior management approval for establishing business relationships with PEPs alongwith evaluation of Compliance officer and Principal officer. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, we need to obtain senior management approval to continue the business relationship.
11. Take reasonable measures to verify sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
12. In case of failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary
13. Following clients are considered to the Clients of Special Category (CSC) for whom enhanced care would need to be taken in the due diligence process of such high-risk clients.
 - a. Non-resident clients,
 - b. High Net-worth Individuals,
 - c. Trusts, Charities, NGOs and organizations receiving donations,
 - d. Companies having close family shareholding or beneficial ownership,
 - e. Politically Exposed Persons (PEP) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The additional norms applicable to PEP as enumerated above shall also be applied to the accounts of the family members or close relatives of PEPs. Re-check for PEP definition
 - f. Companies offering foreign exchange offerings
 - g. Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information.

RISK MANAGEMENT

1. **Risk Based Approach:** Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. These parameters should 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 KYC profile on best effort basis. In line with the risk- based approach, type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

2. **Risk Assessment** : We 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. 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. The assessment where applicable may be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

In addition to the above, we shall identify and assess the ML and TF risk that may arise in (relation to the development of new products and new business practices, including new delivery mechanisms, and use of new or developing technologies for both new and existing products. We shall ensure:

1. To undertake the assessments prior to the launch or use of such products, practices, services, technologies; and
2. We shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

TRANSACTION MONITORING

1. Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. We shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The RMS team shall specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. RMS team under online and compliance under offline surveillance keep track of the transactions
2. As a policy, we shall not accept cash from any clients.
3. The Principal Officer, by himself and his team or through the Compliance and Surveillance team, arrange to review selection of transactions undertaken by clients so as to check if there are any suspicious transactions
4. We may specify threshold limits for client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to regulators during audit, inspection or as and when required.
5. We 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
6. Compliance and Surveillance team 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. Any transactions needing special attention such as complex transactions, unusually large `transactions / patterns which appear to have no economic rationale etc. shall be brought to the notice of the Principal Officer.
8. Transactions in the nature as below are few examples of suspicious transactions and any such suspicious transaction should be reported immediately to the Money Laundering Control Officer (Principal Officer) mentioned hereunder and his advice taken.
 - a. Clients whose identity/ verification seems difficult or client appears not to cooperate, Portfolio Management services for clients where source of funds is not clear or not in keeping with clients apparent standing / business activity, Clients in high risk jurisdictions or clients introduced by

- intermediaries / referral sources based in high risk jurisdictions Substantial increase in business without apparent cause.
- b. Clients whose identity verification seems difficult or clients that appear not to cooperate
 - c. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
 - d. Clients based in high risk jurisdictions;
 - 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. Requests for transfer of investment proceeds to apparently unrelated third parties, unusual transactions by CSCs and business undertaken by shell corporations, offshore banks / financial services, business reported in the nature of export-import of small items, etc.
9. Record of all transactions and KYC documents collected from the Clients shall be maintained at least for such period as prescribed under the relevant Regulations. Attempt shall be made to maintain electronic scanned copies of client documentation.
 10. We 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.
 11. We shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.
 12. In case of 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:
 - 1)the origin of the funds
 - 2)the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
 - 3)the identity of the person undertaking the transaction;
 - 4)the destination of the funds;
 - 5)the form of instruction and authority.
 13. We shall ensure that 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 period which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations

RETENTION OF RECORDS

1. We shall maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:
 - a. the nature of the transactions;
 - b. the amount of the transaction and currency in which it is denominated;
 - c. the date on which the transaction was conducted; and
 - d. the parties to the transaction
2. We 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. Records evidencing the identity of its clients and beneficial owners as well as records and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and us 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 shall be retained until it is confirmed that the case has been closed.

3. We shall need to 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 us and the client
4. More specifically, we need to ensure and place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below :
 - a. All cash transactions of the value more than Rs. 10 lacs or its equivalent in foreign currency
 - b. All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lacs or its equivalent in foreign currency where such series of transactions take place within one calendar month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency.
 - c. 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 us.
 - d. For the purpose of suspicious transactions reporting, apart from transactions integrally connected, transactions remotely connected or related are also to be considered.
 - e. Where we do not have records of the identity of its existing client, it shall obtain the records forthwith, failing which, we shall close the account of the client, after giving due notice to the client.

Procedure for freezing of funds, financial assets or economic resources or related services : In terms of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (“WMD Act”), the Central Government is empowered as under: For prevention of financing by any person of any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to a) Freeze, seize or attach funds or other financial assets or economic resources— i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or ii. held by or on behalf of, or at the direction of, such person; or iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person; b) prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems. The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7 of the Act.

The obligations to be followed by us to ensure the effective and expeditious implementation of the said order has been issued vide SEBI Master Circular ref. no.: SEBI/ HO/ MIRSD/ MIRSD-SEC-5/P/CIR/2023/022 dated 3rd February 2023; Further, SEBI’s circular no. EBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated 16th June 2023 needs to be complied with the circulars and guidelines issued by the Regulators/Exchanges and other law enforcement agencies.

Procedure for unfreezing of funds, financial assets or economic resources or related services: If individuals or entities have the evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them have been inadvertently frozen, shall move an application giving the

requisite evidence, in writing to the concerned stock exchanges/depositories and UAPA Nodal Officer of State/UT.

As a Member, we shall inform and forward a copy of the application together with full details of the asset(s) frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services frozen inadvertently to the appropriate authorities within the prescribed time limit. In order to ensure the expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated 2nd February 2021 for strict compliance. These guidelines have been further amended vide a Gazette Notification dated 8th June 2021 and a corrigendum dated 15th March 2023 (Page 4 of 4) has also been issued in this regard - Mentioned in SEBI Circular SEBI/ HO/ MIRSD/ MIRSD-SEC-5/P/CIR/2023/022 dated 3rd February 2023 and SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated 16th June 2023.

5. Procedure for freezing of funds, financial assets or economic resources or related services : The Stock exchanges and the registered intermediaries shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do 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). In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021

REPORTING OF TRANSACTIONS

1. In terms of the PML Rules, we are required to report we are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at their given address and upload report under appropriate login id's created with FIU-IND created for its various memberships
2. Although detailed instructions for filing these reports are given in the instructions part of the related formats and we need to adhere to the following:
 - a. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month; however, since we do not undertake cash transactions, CTR is not applicable to us.
 - b. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
 - c. The Non Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month. We keep a track of the transactions done by Non Profit Organization / Public Trusts accounts maintained with us every month and accordingly evaluate the same.
3. The Principal Officer will be responsible for timely submission of STR and NTR to FIU-IND;
4. Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND. No Nil reporting needs to be made to FIU-IND in case there are no suspicious/ non – profit organization transactions to be reported. For the accounts which are been reported to FIU-IND as STR, no restrictions are to be placed on operations of the said accounts and no information about the same should be disclosed (“tip-off”) to the client at any level.

CO-OPERATION WITH AUTHORITIES

1. The Company and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining client confidentiality. Confidential information about clients may, therefore, only be given to the authorities when there is a legal obligation to do so.
2. The Company and its staff shall strictly ensure that there is no 'tipping-off' to clients about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a client, it may seriously hamper the enquiry/investigation of the authorities.
3. There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases, the Company would cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

HIRING AND TRAINING PROCESS

1. Hiring of Employees: Identify need for a new or replacement of a particular position, in co-ordination the Concerned Head of department (HOD) define job description and salary range for the position. HR team shall request on job portals and approaches placements for on time recruitment. The applications of candidates are reviewed, identified candidates are evaluated, If found suitable, profile of said candidates referred to concerned head of department for review, shortlisted profiles are scheduled interview for further assessment. The shortlisted candidates which are above managerial position and /or positions which are directly involved with client interface, shall be called upon to meet senior management for evaluation. The selected candidate are proceeded for recruitment, only after a proper reference check with previous employer and one personal contact and submission of documents like., Address proof, previous employer salary slip , reliving letter Pan Card etc., required information and supporting documents. Credential evaluations is done through watchout investor.com.If found appropriate an offer letter is issued and same is accepted by candidate further onboarding process happens wherein supporting documents such as id proof, education proof are verified in originals, explained about the company polices etc Also for the key positions within the organization, we ensure that they are suitable and competent to perform their duties.
2. Employees' Training: VRM Share Broking Private Limited will on an ongoing basis arrange and organize for employee training programme for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers, so that the employees are adequately trained in AML and CFT procedures, and that that they understand the rationale behind these guidelines, obligations and requirements.

DESIGNATED DIRECTOR/ PRINCIPAL OFFICER / MONEY LAUNDERING CONTROL OFFICER/S

To ensure that we properly discharge the legal obligations to report suspicious transactions to the authorities, the Designated Director and 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.

The Designated Director and Principal Officer appointed by the Company shall be responsible for the following:

- a. Communicating the Policy on Prevention of Money Laundering to the employees of respective companies
- b. Receiving reports from employees for any suspicious dealings noticed by them
- c. Clarifying any queries from employees on this matter
- d. Ensuring that the employees dealing with the clients / prospective clients are aware of the KYC guidelines of the Company and are advised to follow the same strictly
- e. Conduct a sample test of client dealings, by themselves or through an internal audit process, to satisfy them that no suspicious activities exist
- f. Report any suspicious transactions to appropriate authorities

REVIEW OF POLICY

The directives issued by the regulators would be adopted by the entity from time to time, but the same would be incorporated in this policy during its review. In view of which this policy document would be subject to review on periodical basis viz. annually and/or in case of any major regulatory directives.