****

MY MONEY SECURITIES LIMITED

H.O.: 10-A UNDER HILL LANE,
CIVIL LINES, DELHI-110054

****

Policy created by : Mr. Pawan Chawla	Operational staff and Compliance Officer
Policy reviewed by : Vikas Seth	Policy reviewed on : 31.03.2025
Approval authority : MMSL Management	Managing Director – Mr. Sanjai Seth
Policy approved on : 31.03.2025	Previous Review : 30.09.2024
Periodicity of Review periodicity : HalfYearly	Last reviewed on : 31.03.2025
Version number : 2.3	Policy on Website : Yes

ANTI MONEY LAUNDERING POLICY

The Government of India has serious concerns over money laundering activities which are not only illegal but anti-national as well. As a market participant it is evident that strict and vigilant tracking of all transactions of suspicious nature required.

Accordingly the Company has laid down following policy guidelines: Principal Officer:

Mr. Sanjai Seth, is appointed as the Principal Officers for Trading & DP operations. He will be responsible for implementation of internal controls & procedures for identifying and reporting any suspicious transaction or activity to the concerned authorities.

Internal Policies, Procedures and Controls:

Company has adopted written procedures to implement the anti-money laundering provisions as envisaged under the Anti-Money Laundering Act, 2002. Such procedures should include inter alia, the following three specific parameters which are related to the overall.

Client due diligence process:

Policy for acceptance of clients Procedure for identifying the clients Transaction monitoring

and reporting especially Suspicious Transactions Reporting (STR)

1. **Customer Due Diligence**

The customer due diligence (<CDD=) measures comprise the following:
Obtaining sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Verify the customer's identity using reliable, independent source documents, data or information;

Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;

Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and

Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactionsand account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediarys knowledge ofthe customer, its business and risk profile, taking into account, where necessary, the customer's source of funds.

1.2 **Policy for acceptance of clients:**

Company develops customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. By establishing such policies and procedures, we will be in a better position to apply customer due diligence on a risk sensitive basis depending on the type of customer business relationship or transaction. In a nutshell, the following safeguards are to be followed while accepting the clients:

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

Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to client's location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, DP turnover etc. andmanner of making payment for transactions undertaken. The parameters will enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile.

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.
Ensure that an account is not opened where the back office and DP staff is unable to apply appropriate clients due diligence measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, information provided to the back office and DP staff is suspected to be non-genuine, perceived non co-operation of the client in providing full and complete information. The back office and DP staff should not continue to do business with such a person and file a suspicious activity report. It should also evaluate whether there is suspicious DP in determining whether to freeze or close the account. The back office and DP staff should be cautious to ensure that it does not return securities of money that may be from suspicious trades. However, the back office and DP staff should consult the relevant authorities in determining what action it should take when it suspects suspicious.

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

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.

1.3 Risk-based Approach

1.3.1 It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, the back office and DP staff should apply each of the customers due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the back office and DP staff should adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers. In line with the risk-based approach, the type and amount of identification information and documents that the back office and DP staff should obtain necessarily depend on the risk category of a particular customer.

1.4 Clients of special category (CSC):

Such clients include the following-

- Non-resident clients High net worth clients,
- Trust, Charities, NGOs and organizations receiving donations

- Companies having close family shareholdings or beneficial ownership
- Politically exposed persons (PEP) of foreign origin
- Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
- Companies offering foreign exchange offerings
- 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.
- Non face to face clients
- Clients with dubious reputation as per public information available etc.

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

1.5 Client identification procedure:

- The KYC /client identification procedures have been specified and strengthened by SEBI from time to time. For example, SEBI vide its circular no. SMD-1/23341 dated November 18, 2003 laid down the mandatory requirement to obtain details of clients by brokers and formats of clients registration form and broker client agreements were specified vide circular no. SMD/POLICY/CIRCULARS/5-97 dated April 11, 1997. Subsequently in order to bring about uniformity in documentary requirements across different segments and exchanges as also to avoid duplication and multiplicity of documents, uniform documentary requirements for trading across different segments and exchanges have been specified vide SEBI circular no/ SEBI/MIRSD/DPS-1/Cir-31/2004 dated August 26, 2004. Similarly KYC circulars with regard to depositories have been issued vide circulars no. SMDRP/Policy/Cir- 36/2000 dated August 04, 2000, circular no. MRD/DOP/Dep/Cir- 29/2004 dated August 24, 2004 and circular no. MRD/DoP/Dep/Cir-12/2007 dated September 7, 2007. Similarly prohibition on acceptance of cash from clients has been specified vide SEBI circular no. SEBI/MRD/SE/Cir-33/2003/27/08 dated August 27, 2003.

- In Order to further strengthen the KYC norms and identify every participant in the securities market with their respective PAN thereby ensuring sound audit trail of all the transactions, PAN has been made sole identification number for all participants transacting in the securities market, irrespective of the amount of transaction vide SEBI Circular reference MRD/DoP/Cir-05/2007 dated April 27, 2007, subject to certain exemptions granted under circular reference MRD/DoP/MF/Cir-08/208 dated April 03, 2008 and MRD/DoP/Cir- 20/2008 dated June 30, 2008.

- All The back office and DP staff should put in place necessary procedures to determine whether their existing/potential customer is a politically exposed person

(PEP). Such procedures would include seeking additional information from clients, accessing publicly available information etc.

- All The back office and DP staff are required to obtain senior management approval forestablishing business relationships with Politically Exposed Persons. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, The back office and DP staff shall obtain senior management approval to continue the business relationship.

- The back office and DP staff shall take reasonable measures to verify source of funds ofclients identified as PEP.

- The client should be identified by the back office and DP staff by using reliable sources including documents / information. The back office and DP staff should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

The information should be adequate enough to satisfy competent authorities (regulatory/ enforcement authorities) in future that due diligence was observed by the intermediary in Compliance with the Guidelines. Each original documents are should be seen prior to acceptanceof a copy.

- Failure by prospective client to provide satisfactory evidence of identity should be notedand reported to the higher authority within the intermediary.

- SEBI has prescribed the minimum requirements relating to KYC for certain class of the back office and DP staff from time to time as stated earlier in this para . Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, all the back office and DP staff should frame their own internal guidelines based on their experience in dealing with their clients and legal requirements as per the established practices. Further, the back office and DP staff should also maintain continuous familiarity and follow-up where it notices inconsistencies inthe information provided. The underlying objective should be to follow the requirements enshrined in the PML Act, 2002 SEBI Act, 1992 and Regulations, directives and circulars issued thereunder so that the back office and DP staff is aware of the clients on whose behalf it is dealing.

- Company will formulate and implement a client identification programme which shall incorporate the requirements of the Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients. A copy of the client identification program shall be forwarded to the Director, FIU- IND.

- It may be noted that while risk based approach may be adopted at the time of

establishing business relationship with a client, no exemption from obtaining the minimum information/documents from clients as provided in the PMLA Rules is available to brokers in respect of any class of investors with regard to the verification of the records of the identity of clients.

2. Record Keeping

The back office and DP staff should ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

The back office and DP staff should maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, the back office and DP staff should retain the following information for the accounts of their customers 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 selected transactions:
- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

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

More specifically, the back office and DP staff shall put in place a system of maintaining proper record of transactions prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002 as mentioned below:
All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

- All series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;.

- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

3. Information to be maintained

Company will maintain and preserve the following information in respect of transactions referred to in Rule 3 of PMLA Rules:
The nature of the transactions;

- the amount of the transaction and the currency in which it denominated; the date onwhich the transaction was conducted; and
- The parties to the transaction.

4. Retention of Records

The back office and trading staff should 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. Further, the records mentioned in Rule 3 of PMLA Rules have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

As stated in para 1.5, The back office and trading staff are required to formulate and implement the client identification program containing the requirements as laid down in Rule 9 and such other additional requirements that it considers appropriate. The records of the identity of clients have to be maintained and preserved for a period of eight years from the date of cessation of the transactions between the client and intermediary.

Thus the following document retention terms should be observed:

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

Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the same period.

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

5. Monitoring of transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the Anti-MoneyLaundering procedures. This is possible only if the back office and DP staff has an understanding of the normal activity of the client so that they can identify the deviant transactions / activities.

The back office and trading staff should pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. The back office and DP staff may specify internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these limits.

The back office and trading staff should ensure a record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section
12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.

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

6. Suspicious Transaction Monitoring & Reporting

The back office and trading staff should ensure to take appropriate steps to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, intermediaries should be guided by definition of suspicious transaction contained in PML Rules as amended from time to time.

A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

- Clients whose identity verification seems difficult or clients appears not to cooperate
- Asset management services for clients where the source of the funds is not clear ornot in keeping with clients apparent standing /business activity;
- Clients in high-risk jurisdictions or clients introduced by banks or affiliates or otherclients based in high risk jurisdictions;
- Substantial increases in business without apparent cause;
- Unusually large cash deposits made by an individual or business;
- Clients transferring large sums of money to or from overseas locations withinstructions for payment in cash;
- Transfer of investment proceeds to apparently unrelated third parties;
- Unusual transactions by CSCs and businesses undertaken by shell

corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicion transaction should be immediately notified to the Money Laundering Control Officer or any other designated officer within the intermediary. The notification may be donein the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

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

7. Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU- IND)at the following address:
Director, FIU-IND,

Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi -110021.

Website: https://www.fingate.gov.in/

The back office ~~and trading staff should carefully go thr~~ough all the reporting requirements and formats enclosed with this circular. These requirements and formats are divided into two parts- Manual Formats and Electronic Formats. Details of these formats are given in the documents (Cash Transaction Report- version 2.0 and Suspicious Transactions Report version 2.0) which are also enclosed with this circular. These documents contain detailed guidelines on the compilation and manner/procedure of submission of the manual/electronic reports to FIU- IND. The related hardware and technical requirement for preparing reports in manual/electronic format, the related data files and data structures thereof are also detailed in these documents. If not in a position to immediately file electronic reports, may file manual reports to FIU-IND as per the formats prescribed. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, the back office and DP staff should adhere to the following:

The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.

The Suspicious Transaction Report (STR) should 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 should record his reasons for treating any transaction or series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.
The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND; Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

The back office and DP staff should not put any restrictions on operations in the accounts where an STR has been made. The directors, officers and employees (permanent and temporary) should be prohibited from disclosing (<tipping off=) the fact that a STR or related information is being reported or provided to the FIU-IND. Thus, it should be ensured that there is no tipping off to the client at any level.

8. Designation of an officer for reporting of suspicious transactions

8.1 To ensure that the back office and DP staffs properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions. Names, designation and addresses (including e-mail addresses) of 8Principal Officer9 including any changes therein shall also be intimated to the Office of the Director- FIU. As a matter of principle, it is advisable that the 8Principal Officer9 is of a sufficiently higher position and is able to discharge his functions with independence and authority.

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

9.1 Hiring of Employees

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

9.2 Employees' Training

Company must have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements should have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their

systems being misused by unscrupulous elements.

9.3 Investors Education

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

10. List of key circulars issued with regard to KYC/AML/CFT

	Circular No.	Date of circular	Subject	Broad area covered
	MRD/DoP/Cir-05/2007	April 27, 2007	PAN to be the Sole identification number for all transactions in the securities Market	In order to strengthen KYC and identify every participant in the securities market with the irrespective PAN, so as to ensure sound audit trail, PAN made mandatory for participants transacting in the securities market.
	ISD/CIR/RR/AML/2/06	March 20, 2006	Prevention of Money Laundering Act, 2002- Obligations of intermediaries in terms of Rules notified there under	Procedure for maintaining and preserving records, reporting requirements and formats of reporting cash transactions and suspicious transactions
	ISD/CIR/RR/AML/1/06	January 18, 2006	Guidelines on Anti-Money Laundering Standards	Framework for AML and CFT including policies and procedures, Customer Due Diligence requirements, record keeping, retention, monitoring and reporting
	SEBI/MIRSD/DPS-1/Cir-31/2004	August 26, 2004	Uniform Documentary Requirements for DP	Uniform KYC documentary requirements for DP on different segments and Exchanges

	MRD/DoP/Dep/Cir-29/2004	August 24, 2004	Proof of Identity (POI) and Proof of Address (POA) for opening a Beneficiary Owner (BO) Account for non-body corporate	Broadening the list of documents that may be accepted as Proof of Identity(POI) and/or Proof of Address (POA) for the purpose of opening a BO Account
	SEBI/MRD/SE/Cir-33/2003/27/08	August 27, 2003	Mode of payment and delivery	Prohibition on acceptance/giving of cash by brokers and on third party transfer of securities
	SMD/POLICY/CIRCULARS/5-97	April 11, 1997	Client Registration Form	Formats of client Registration Form and broker clients agreements
	SMD-1/23341	Nov. 18, 1993	Regulation of transaction between clients and members	Mandatory requirement to obtain details of clients by brokers.