

ANTI MONEY LAUNDERING POLICY

Prevention of Money Laundering Act, 2002 was notified on July 1, 2005. Subsequent to this, the Securities and Exchange Board of India (SEBI) has on 18th January 2006 (Circular Ref. No. ISD/CIR/RR/AML/1/06) required market intermediaries to adopt a policy framework with respect to Anti Money Laundering measures to be followed by the intermediaries. SEBI vide a Master Circular Ref. No. ISD/AML/CIR-1/2008 dated 19th December 2008 directed all registered intermediaries to ensure compliance with the requirements of the Anti Money Laundering (AML) Standards/ Combating Financing of Terrorism (CFT) / Obligations of the Security Market Intermediaries under Prevention of Money Laundering Act 2002 and rules framed there-under. SIPL is inter alia, a stock broker, a Depository Participant (DP), a registered intermediary with SEBI and needs to adhere to the same.

SIPL has formulated a policy to comply with the SEBI circular. As per the existing policy, SIPL has to monitor, all market and Off-market Transactions, inter depository Transactions and Pledge Invocation cases where total value of a single transaction and or series of transaction in single scrip in a month is greater than Rs. 10 lacs. This policy was framed in December 2006. In the present market scenario, it is not practically possible to report every transaction of value Rs.10 lacs or above. Hence it is felt that we will revise our Anti Money Laundering Policy. Since the business of the SIPL has increased, it is necessary to review the same.

Every transaction in the capital market has two parts i.e. Securities and Funds. It is difficult for SIPL to know about the actual Sources of funds/securities provided to SIPL. Monitoring the exact income and net-worth of clients and comparing their transaction value with their income and net-worth are also difficult. Therefore a policy of reporting suspicious Transactions is required to be framed and implemented.

Objectives:

- To ensure that SIPL meets legal and regulatory obligations, and that its staff is trained properly to adhere and comply with prevalent laid down requirements;
- To establish the process of internal control over clients' trading and Demat accounts and activities falling under the category of suspicious nature by identifying, monitoring and reporting to law enforcement authorities;
- To update all subsequent notifications issued by various regulatory authority/exchanges having relevance to the business of intermediary carried on by SIPL.
- To ensure that the policy/procedures framed are implemented / applied effectively.

Definition of Money Laundering:

Section 3 of PMLA has defined the "**offence of money laundering**" as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

Obligations under Prevention of Money Laundering (PML) Act 2002:

- (I) Anti-Money Laundering Policy should be approved in writing by Board / Senior Management and reviewed at frequent intervals.
- (II) Implementation of the Anti-money Laundering Policy-
PMLA places certain obligations on every banking company, financial institution and intermediary, which include implementation of the Anti-Money Laundering Policy
 - (i) To maintain a record of prescribed transactions
 - (ii) To furnish information of prescribed transactions to the specified authority
 - (iii) To verify and maintain records of the identity of its clients
 - (iv) To preserve records in respect of (i), (ii) and (iii) above for a stipulated period (presently five years) from the date of cessation of transactions with the clients.

Key Elements of the Policy:

The Policy covers the following key areas and defines procedures and measures to be undertaken by the concerned officials.

1. Designation of an officer for reporting of suspicious transactions
2. Customer Due Diligence and freezing of funds, financial assets/services etc.
3. Transaction Monitoring & Record Keeping
4. Maintenance and Perseverance of Records
5. Audit/ testing of Anti-Money Laundering program
6. Reporting to Financial Intelligence Unit (FIU)-India
7. Employees' Hiring and Training
8. Investors' Education

1. CUSTOMER DUE DILIGENCE AND FREEZING OF FUNDS, FINANCIAL ASSETS/SERVICES ETC.

1.1 Customer Due Diligence ("CDD") measures comprise the following:

The concerned official shall obtain sufficient information about the prospective client and follow the Know Your Client (KYC) procedure for in-person verification of client for both the accounts i.e. Demat and Trading. The concerned official shall take special care in case the natural person, who is desirous of opening an account, suggests that someone else will operate the account in his name. The identification process for the ultimate beneficiary or authority controlling the account should be undertaken, as per the prevalent norms as may be applicable.

ANTI MONEY LAUNDERING POLICY

In case of corporate clients or clients being legal person, the identity and beneficial ownership of the legal person should be ascertained and verified. The authorized person being designated to operate the account should also be identified both for beneficial owner entities or group as well as the authorized person.

1.2 Client Identification / Acceptance procedure:

The concerned officials i.e. front office as well as back office executives shall ensure that:

- (1) No account is opened in fictitious or *benami* name or in anonymous manner.
- (2) The senior official shall classify the client into High Risk, Medium Risk and Low Risk category considering the client's location, address, nature of business activity, trading turnover and the manner of making payments.
If a client's profile warrants likelihood of being of high-risk category, immediate attention of the Principal Officer shall be drawn.
- (3) The documents defined and processes prescribed by SEBI/Exchanges, RBI, NSDL/CDSL and the existing management policies are strictly adhered to.
- (4) In case a client is authorizing someone else for operating his account, the same shall be duly recorded with proper process for authorized person. In such cases, a certified true copy of properly executed power of attorney on stamp paper of applicable value must be obtained and the signature as well as details of Power of Attorney should be recorded in the System.
- (5) Sufficient care should be taken to verify past history/track record of the client to ensure that no actions were initiated against him by any regulatory authority or enforcement agency, and that the identity of the client does not match with any person having criminal background or is not banned in any other manner.
- (6) Non-resident clients' registration should be done only after obtaining proper introduction/recommendation from a reliable source like Bank etc.
- (7) A new client should be registered after obtaining introduction from sub-broker or Authorised Person.
- (8) The following classes of clients are defined as "Special Category Clients" (SCC) and the registration is done after more detailed scrutiny and after obtaining reference from a reliable source only.
 - i. Non Resident Clients
 - ii. High net worth Clients
 - iii. Trusts, Charitable Organizations, NGO and organizations receiving donations.
 - iv. Companies having close family shareholdings or beneficial ownership
 - v. Politically Exposed Persons (PEP): Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, as clarified vide SEBI Circular ISD/AML/CIR-1/2009 dated September 01, 2009. This may also include Current or former senior high profile politicians, their family members and connected entities.
 - vi. Companies offering foreign exchange offerings
 - vii. Clients in high risk countries as clarified vide SEBI Circular ISD/AML/CIR-1/2009 dated September 01, 2009
 - viii. Non face to face clients
 - ix. Clients with dubious reputation as per public information available etc.
- (9) Before opening any new account, SIPL shall ensure that the name/s of the proposed customer does not appear in the 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 Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) as available on United Nations website at <https://www.un.org/securitycouncil/content/resolutions> and 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. In case of full details of accounts bearing resemblance with any of the individuals/entities in the list, it would be immediately be intimated to SEBI and FIU-IND.
- (10) The company shall obtain sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

In order to follow uniform approach towards determination of beneficial ownership for clients other than individuals or trusts, viz., Company, Partnership or unincorporated association/body of individuals or for client which is a trust, the company shall take reasonable measures to verify the identity of such persons as per guidelines on identification of beneficial ownership issued by SEBI vide its circular no. CIR/MIRSD/2/2013 dated January 24, 2013.
- (11) Reliance on third party for carrying out Client Due Diligence (CDD)
 - i. The company may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PMLAct.
 - ii. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. The company shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

1.3 Activation in DPM System and Allotment of Demat Account No.:

After completion of Know Your Client (KYC) procedure, the client data shall be entered and authorized in DP system and thereafter activated in DPM System (software provided by NSDL to DP), for allotment of Demat Account Number to the client.

ANTI MONEY LAUNDERING POLICY

1.4 Allotment of UCC:

After completion of Know Your Client (KYC) procedure, Unique Client Code (UCC) is allotted to the client and the same shall be uploaded to the Exchange with Permanent Account Number (PAN).

SEBI vide circular no. SEBI/HO/MIRSD/DOSR1/CIR/P/2018/93 dated 13.06.2018 issued a circular pertaining to amendments to Prevention of Money-laundering (Maintenance of Records) Rules 2005 by Government of India in its various notifications issued on 01.06.2017, 16.10.2017, 23.10.2017, 31.03.2018 mainly pertaining to submission of Aadhaar number; and also clarified that in terms of SEBI circular dated 27.04.2017, the requirement of PAN would continue to be mandatory for completing the KYC process. (Inserted vide dated 29th June 2018)

1.5 Access of Information

The Principal Officer/Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

2. **TRANSACTION MONITORING & RECORD KEEPING**

2.1 All persons associated with operations, risk management and back office operations, either Broking or DP shall take due care and report any transaction which is felt to be of suspicious nature on any ground, shall alert the Principal Officer through his immediate reporting authority. The following illustrations would explain the basic approach.

1. *Unusually large transactions / patterns which appear to have no economic purpose.*
2. *Off market transactions with other beneficiary account holders having no reasonable grounds.*
3. *Clients whose identity verification is difficult or clients that appear not to cooperate*
4. *Substantial increase in activity without apparent cause*
5. *Sudden activity in dormant account*
6. *Suspicious off market transactions*
7. *Large deals at prices away from the market*
8. *Large number of accounts having common parameters such as common partner/ directors/ addresses, email address, telephone number/ introducers or authorized signatories.*
9. *Unusual unique client code change activity with no proper justification in respect of market trades*
10. *Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;*
11. *Clients based in high risk jurisdictions;*
12. *Substantial increases in business without apparent cause;*
13. *Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;*
14. *Attempted transfer of investment proceeds to apparently unrelated third parties;*
15. *Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export- import of small items.*
16. *All suspicious off market transactions other than those appearing in Depository alerts, (as reviewed in board meeting held on 18th March 2017)*

2.2 High value transactions shall be identified for review by appropriately authorized back office executive and any transaction of suspicious nature shall be immediately intimated to Principal Officer.

2.3 The officials associated with front desk and risk management and back office shall ensure that

1. All sub-brokers/authorized persons/clients are given a limit on either mark to market loss, gross exposure etc. parameters based on their balances available with the company. The sub-brokers /authorized persons shall be responsible for deciding trading limits for their respective clients.
2. No cash transactions with the client to be undertaken.
3. Cheques and securities received from client shall have to be from his pre-declared bank account and demat account. In case on non-compliance, shares or moneys, as the case may be, be returned to the account from where it has come from and the relationship terminated after closing out all transactions in accordance with provisions in this regard.
4. Illiquid contracts in F&O segments shall not be allowed to all clients.

2.4 Clients of high risk countries shall be subject to appropriate counter measures, in respect of further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

The company shall endeavor to 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 SIPL and its sub-broker's /authorized person's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

2.5 The company shall ensure expeditious and effective implementation of the procedure laid down in the UAPA Order dated 27th August 2009 regarding prevention of certain unlawful activities of individuals and associations and for matters connected therewith.

ANTI MONEY LAUNDERING POLICY

- 2.6 Where upon receipt of the updated list of designated individuals / entities either from SEBI or Exchange or depositories, the company shall comply with the provisions of SEBI circular ISD/AML/CIR-2/2009 dated 23rd October 2009 including freezing/unfreezing of financial assets, economic resources or related services and intimate to relevant authorities.
- 2.7 The internal audit or compliance function shall also endeavor to ensure compliance with the policies, procedures, and controls relating to the 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. Further, the internal audit function shall be independent, adequately resourced and commensurate with the size of business and operations, organization structure, number of clients and other such factors.
- 2.8 Risk-based Approach**
 Certain clients may be of a higher or lower risk category depending on circumstances such as the client's background, type of business relationship or transaction etc. and so, SIPL shall endeavor to apply each of the clients due diligence measures on a risk sensitive basis. The risk categorization as reviewed by the Board of Directors in its meeting held on 26.08.2016 may be guided as per Annexure I of this policy
- SIPL shall endeavor to adopt an enhanced client due diligence process for higher risk categories of client and a simplified client due diligence process for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that the company shall obtain necessarily depend on the risk category of a particular client. However, low risk approach shall not apply when there are suspicious of ML/FT or when other factors give rise to a belief that the customer does not in fact pose low risk.
- While dealing with clients in high risk countries where existence/effectiveness of money laundering control is suspect, The Company shall independently access and consider other publicly available information, 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 <https://www.fatf-gafi.org/>
- The company shall endeavor to put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person, which may include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS and that the enhanced CDD measures shall be applied where the beneficial owner of a client is a PEP, and take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
- 2.9 Risk Assessment**
 i. The company shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions which can be accessed at <https://www.un.org/securitycouncil/content/resolutions>
- ii. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.
- 2.10 The company shall pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. SIPL may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/office records / memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI /stock exchanges/FIU-IND/other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for five years from the date of transaction between the client and the company.
- 2.11 Further, concerned department of the company shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not. Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer or any other designated officer in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it would be ensured that there is continuity in dealing with the client as normal until told otherwise and the client would not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Principal Officer/Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

ANTI MONEY LAUNDERING POLICY

3. MAINTENANCE AND PRESERVANCE OF RECORDS

SIPL shall maintain all records and documents prescribed under the applicable laws, rules, regulations, byelaws, circulars and guidelines etc. The officials shall ensure that the records are kept in an easily accessible manner so that it shall be available as and when required by the relevant authorities.

- 3.1 The company 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. Further, the records mentioned in Rule 3 of PML Rules as amended, have to be maintained and preserved for a period of five years from the date of transactions between the client and the company.
- 3.2 SIPL shall formulate and implement the client identification procedure (CIP) containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Further, records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and the company has ended or the account has been closed, whichever is later.
- 3.3 All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA and rules framed thereunder as well SEBI Act) and other legislations, Regulations or exchange bye-laws or circulars.
Further, Records on client identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence shall also be kept for the same period.
- 3.4 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.
- 3.5 The company shall maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the company.
- 3.6 The identification documents and other details should be periodically updated either on quarterly or annually, including all documents, data or information of all clients and beneficial owners collected under the customer due diligence process, and that customer due diligence process shall be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).
- 3.7 Changes required in client bank details and address details pursuant to requests received in properly filled modification form with sufficient proofs should be incorporated in records/database and the same to be retained with client identification documents.

4. REPORTING TO FINANCIAL INTELLIGENCE UNIT (FIU)-INDIA

SIPL shall report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address; or to the address which may prescribe hereafter:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri, New Delhi
110021
Website: <https://fiuindia.gov.in>

Type of information required to be furnished:

Every banking company, financial institution and intermediary is required to furnish information about –

- all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- 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;
- all suspicious transactions whether or not made in cash. It is clarified that “SIPL, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, can file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.”

Time limits prescribed for furnishing information to Director, FIU-IND:

- Rule 8 of the Rules notified by Notification No.9/2005 (as amended by Notification No.15/2005 and 4/2007) prescribes time limit for furnishing information to the Director, FIU-IND.
- The time limit for furnishing information about cash transactions and integrally connected cash transactions to Director, FIU-IND is 15th day of the succeeding month.
- 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 should be furnished to the Director, FIU-IND not later

ANTI MONEY LAUNDERING POLICY

than seven working days from the date of occurrence of such transactions.

- All suspicious transactions have to be furnished to the Director, FIU-IND not later than seven working days on being satisfied that the transaction is suspicious.

5. DESIGNATION OF AN OFFICER FOR REPORTING OF SUSPICIOUS TRANSACTIONS

SIPL shall appoint the Principal Officer who would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in identification and assessment of potentially suspicious transactions. Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-Financial Intelligence Unit (FIU). The Principal Officer shall have access to and be able to report to senior management above his/her next reporting level or the Board of Directors.

In addition to the existing requirement of designation of a Principal Officer, SIPL shall also designate a person as a 'Designated Director' to ensure overall compliance of PMLA requirements.

6. EMPLOYEES' HIRING AND TRAINING

6.1 Hiring of Employees

SIPL shall have adequate screening procedures in place to ensure high standards when hiring employees. It shall identify the key positions within the SIPL's structure having regard to the risk of money laundering and terrorist financing.

6.2 Employees' Training

SIPL shall have an ongoing employee-training program so that the members of the staff are adequately trained in Anti Money Laundering and Combating Financing of Terrorism procedures.

7. INVESTORS' EDUCATION

SIPL shall prepare specific literature so that the clients can be educated on the objectives of the Anti Money Laundering (AML)/Combating Financing of Terrorism (CFT) program.

8. AUTHORISED PERSON TRAINING, AWARENESS FOR IMPLEMENTATION OF ANTI MONEY LAUNDERING POLICY

- 8.1 SIPL shall see that all its sub-brokers/Authorized Persons should adopt Anti-Money Laundering Policy and comply with the requirements

- 8.2 The sub-brokers/Authorized Persons shall submit an undertaking for complying with PMLA requirements. The format of undertaking is attached as Annexure-II.

The Board of Directors in their meeting held on 27th August, 2019 reviewed the aforesaid policy in view of SEBI vide master circular no. SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2018/ 104 dated 04th July 2018 and mentioned that the policy is further subject to review, from time to time in line with regulatory requirements.

The Board further reviewed the policy on 10th December, 2019 in view of SEBI vide master circular no. SEBI Master Circular no. SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113 dated October 15, 2019 regarding guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under and decided that PMLA policy of the company shall be read with provisions of recent SEBI master circular dated October 15, 2019.

LIST OF ABBREVIATIONS USED

- Saurin Investments Pvt. Ltd. : SIPL
- Anti Money Laundering : AML
- Combating Financing of Terrorism : CFT
- Prevention of Money Laundering (PML) Act : PMLA
- Financial Action Task Force : FATF
- Money Laundering Or Financing Of Terrorism : ML/FT
- Customer due diligence : CDD
- Client Identification Procedure : CIP
- Special Category Clients : SCC
- Know Your Client : KYC
- Unique Client Code : UCC
- Permanent Account Number : PAN
- Financial Intelligence Unit-India : FIU-IND
- Depository Participant : DP

REFERENCE

1. Prevention of Money Laundering Act 2002
2. SEBI Circular Ref no. ISD/CIR/RR/AML/1/06 dated January 18, 2006 providing 'Guidelines on Anti Money Laundering Standards'

ANTI MONEY LAUNDERING POLICY

3. SEBI Master Circulars Ref no. ISD/AML/CIR-1/2008 dated December 19, 2008 and CIR/ISD/AML/3/2010 on Anti Money Laundering (AML) Standards/Combating Financing of Terrorism (CFT)/Obligations of Securities Market Intermediaries under Prevention of Money Laundering Act, 2002 and Rules framed there-under-Master Circular on AML/CFT
4. SEBI Circulars dated 1.09.2013, 23.10.2009, 14.06.2010, 22.08.2011, 24.01.2013 and 12.03.2014.
5. SEBI Circular no. SEBI/HO/MIRSD/DOSR1/CIR/P/2018/93 dated 13.06.2018
6. SEBI Master Circular no. SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113 dated October 15, 2019

ANNEXURE - 1

RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF INDIVIDUALS

Type	Recommended Categorization	Risk Perception
Salaried	Low risk	Source on income is fixed and pattern of entries in the account can be correlated with known sources of income/ expenditure.
Senior citizens	Medium Risk / High Risk	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O
House-wife	Medium / High Risk	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O
Self Employed Professionals/ Businessmen	Low risk (except professionals associated with the film industry who will be categorized as "Medium" risk).	Accounts maintained by Chartered Accountants, Architects, Doctors, Lawyers, Sportsmen, etc.
Non Resident Individuals	Medium risk	Transactions are regulated through Authorized Dealers and the accounts are opened only after IPV. In case an IPV is not performed and we have relied on documentation submitted by the client, the account would be categorized as medium risk.
Politically Exposed Persons resident outside India	High Risk	Politically exposed persons 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. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Front end staff should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Such accounts should be subjected to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members and close relatives of PEPs. Further the company may maintain a list of additional accounts as "Designated PEP" The accounts of Politically Exposed Persons resident outside India shall be opened only after obtaining the approval of Business Head. Further, in the event of an existing customer or the beneficial owner of an account subsequently becoming PEP, Business head approval would be required to continue the business relationship and such accounts would be subjected to Customer Due Diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. In such events the company shall be guided by the information provided by the clients or front end teams.

NOTE: If any of the above accounts are operated by Power of Attorney (POA) holder/mandate holder, then the account will be categorized as "High Risk".

ANTI MONEY LAUNDERING POLICY

RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF NONINDIVIDUALS

Risk categorization of Non Individual customers can be done on the basis:

A. Type of Entity B. Industry; C. Country of Domicile

A. Type of Entity

Type	Recommended Risk Categorization	Risk Perception
Private Ltd. /Public Ltd. Companies	Low / Medium / High risk	Depending on the clarity of the shareholding structure and the nature of operations, such companies would be classified.
Local Authorities or Public Bodies	Low Risk	These types of entities are governed by specific Acts, Notifications etc framed by the Government of India or the State Govt. and are controlled and run by the Govt.
Mutual Funds/Scheduled Commercial Banks/Insurance Companies/Financial Institutions	Low Risk	These entities are strictly regulated by their respective regulators.
Partnership Firm	Low / Medium / High risk	Depending on the clarity of the shareholding structure and the nature of operations, such entities would be classified. Such classifications shall be decided post the review of the Department Heads
Trusts – Public Charitable Trust	Medium / High Risk	Depending on the clarity of the beneficial ownership and the nature of operations, such entities would be classified. Such classifications shall be decided post the review of the Department Heads
Hindu Undivided Family (HUF)	Medium Risk	These are unregistered bodies and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.
Societies / Associations /Clubs	High Risk (except 'Housing Societies' which will be categorized as "Low" risk).	These are not highly regulated entities and the pattern of entries in the account may not be correlated with known sources of income/expenditure.
Trusts – Private Trust	High Risk	These may be unregistered trusts and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.
Co-operative Banks	High Risk	These are not highly regulated entities.

B & C. Basis Industry and Country of Domicile

Risk Category	Industry	Country of Domicile
High / Medium / Low	The Risk categorization is dependent on industries which are inherently High Risk or may exhibit high cash intensity, as below: Arms Dealer Money Changer Exchange Houses Gems / Jewelry / Precious metals / Bullion dealers (including sub-dealers) Real Estate Agents Construction Offshore Corporation Art/antique dealers Restaurant /Bar /casino/night club Import/Export agents (traders; goods not used for own manufacturing /retailing) Share & Stock broker Finance Companies (NBFC) Transport Operators Auto dealers (used/ reconditioned vehicles /motorcycles) Scrap metal dealers Liquor distributorship Commodities middlemen Co-operative Banks Car/Boat/Plane dealerships/brokers Multi Level Marketing (MLM) Firms and All other industries	

Notes:

- Higher Risk Categorization derived from either A or B or C shall be the applicable risk categorization for the account.
- Lowering of risk classification shall be carried out by the Compliance officer in consultation with the Department Heads. This shall be done only where adequate justifications can be provided and the same are mentioned along with the account opening form.
- Such justifications shall be reviewed 3 months from the date of account opening / first transaction in order to ensure that the classification is proper.