PREVENTION OF MONEY LAUNDERING (PML) POLICY

1. INTRODUCTION

This Policy has been framed by Yashwi Securities Private Limited ("the Company") in order to comply with the applicable Anti Money Laundering Standards and to take measures to prevent the company from being used as a vehicle for Money Laundering and Terrorist Financing.

Money Laundering and Terrorist Financing

Money laundering is the process by which the illegal origin of wealth is disguised to avoid suspicion of law enforcement authorities and to wipe out the trail of incriminating evidence.

Terrorists and terrorist organisations though may not be keen to disguise the origin of their money but would be interested in concealing the destination and the purpose for which the money is collected. Therefore, terrorists and terrorist organization could also employ techniques to hide and disguise money. Governments around the world recognize the corrosive dangers that unchecked money laundering poses to their economic and political systems and have prescribed acts, rules and regulation for prevention of money laundering.

Need for this Policy

In India, The Prevention of Money Laundering Act, 2005 forms the core of the legal framework to combat money laundering and terrorist financing in India. The Prevention of Money Laundering Act, 2005 came into effect from 1st July 2005 and has been amended on various occasions since.

The Prevention of Money Laundering Act, 2005 imposes an obligation on every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under Section 12 of the SEBI Act) , to verify the identity of investors and maintain records of transactions as specified in the Prevention of Money Laundering Act, 2005 and the Rules, Regulations and Notifications thereunder.

Pursuant to the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering standards, The Securities and Exchange Board of India, has from time to time issued circulars directing

Intermediaries to adopt Strict Customer Due Diligence practices in order to prevent Money Laundering.

Yashwi Securities is an intermediary in the securities market registered with the Securities and Exchange Board of India as a Stock Broker, and a Depository Participant and is thus required to adopt and implement a policy for Prevention of Money Laundering pursuant to the Prevention of Money Laundering Act, 2005 and the Rules, Regulations and Notifications thereunder.

2. POLICY OBJECTIVES:

This Policy aims to achieve the following objectives:

- To protect the Company from being used as a vehicle for money laundering/terrorist financing
- To follow thorough "Know Your Customer" (KYC) policies and procedures in the course of day-to-day business.
- To take appropriate action, once suspicious activities are detected, and report them to the designated authorities in accordance with applicable law / laid down procedures.
- To comply with applicable laws as well as norms adopted internationally with reference to Money Laundering.

3. APPLICABILITY:

This Policy applies to all employees of Yashwi Securities including employees at Corporate Office and Branches.

Applicability of this Policy to various verticals/business of Yashwi Securities

(i) **Institutional Broking**

Appropriate Customer Due Diligence shall be carried out in respect of all Institutional Clients whether registered with SEBI or not. Further, trades of such clients shall be monitored and suspicious transactions, if any, shall be duly reported in accordance with this Policy.

(ii) **Retail Broking**

KYC norms as specified by SEBI/ Exchanges should be adhered to before enlisting clients. Further, trades of such clients shall be monitored and suspicious transactions, if any, shall be duly reported in accordance with this Policy.

(iii) **Depository Participant Activities**

The Depository activity shall be covered within the purview of this Policy. Necessary Customer Due Diligence shall be undertaken. KYC norms as specified by the Depository should be followed for opening accounts. Alerts as generated by the Depositories shall be reviewed and suspicious transaction, if any, shall be duly reported.

4. IMPLEMENTATION OF THIS POLICY

This policy has taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed Directives have outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. Each intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.

Each registered intermediary shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following four specific parameters which are related to the overall 'Client Due Diligence Process':

(i) Policy for acceptance of Clients;

(ii) Procedure for identifying the clients;

(iii) Risk Management;

(iv) Monitoring of Transactions.

Client Due Diligence (CDD)

A. The CDD measures comprise the following:

i) Obtaining 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;

ii) Verify the client's identity using reliable, independent source documents, data or information;

iii) 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 -

a) **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, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

aa) 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 owner-ship of

entitlement to:

(i) more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
(ii) more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
(iii) 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.

bb) In cases where there exists doubt under clause (aa) 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.

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

b) **For client which is a trusts:** Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the author 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;

c) **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;

d) The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

iv) 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 (iii);

v) Understand the ownership and control structure of the client;

vi) 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;

vii) Registered intermediaries shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data; and

viii) Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

Policy for acceptance of clients

All registered intermediaries shall develop client acceptance policies and procedures that aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF. By establishing such policies and procedures, they will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. In a nutshell, the following safeguards are to be followed while accepting the clients:

i. No registered intermediary shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified;

ii. 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. The parameters shall 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 Know Your Client (KYC) profile;

iii. The registered intermediaries shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

a) Non - resident clients;

b) High net-worth clients;

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

d) Companies having close family shareholdings or beneficial ownership;

e) Politically Exposed Persons (PEP). 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 contained in the subsequent paragraph 14 of this circular shall also be applied to the accounts of the family members or close relatives of PEPs;

f) Clients in high risk countries. While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e.

places where existence or effectiveness of action against money laundering or terror financing is suspect, registered intermediaries apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas;

g) **Non face to face clients:** Non face to face clients means clients who open accounts without visiting the branch/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video based customer identification process is treated as face-to-face onboarding of clients;

h) Clients with dubious reputation as per public information available etc;

The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

iv. Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

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

vi. The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall 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 intermediary, as well as the person on whose behalf the agent is acting shall

be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

vii. 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.

viii. The CDD process shall necessarily be revisited when there are suspicions of ML/TF.

Client identification procedure

The KYC policy shall clearly spell out the client identification procedure (CIP) to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

Registered intermediaries shall be in compliance with the following requirements while putting in place a CIP:

i. All registered intermediaries shall proactively 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. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.

ii. All registered intermediaries are required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

iii. Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

iv. The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

v. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.

vi. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

Every intermediary shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules 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.

Risk Categorization And Risk Assessment

Risk-based Approach

All clients should be categorized on the basis of the risk of money laundering or terrorist financing that they are likely to pose. The clients can be classified into the medium or high risk category depending on various criteria like Client wise Large Turnovers, particular Script exposure / trading, client's income range, trading pattern, client is of special category. If any of the client would satisfy the above criteria, depending on the criteria satisfied the same would be classified into medium or high risk.

Clients should broadly be classified in the following categories:

Low Risk	Clients who pose low or nil risk. They are clients who have a respectable social and financial standing. Clients who fulfill obligations on time.
Medium Risk	Intraday clients or speculative client.
High Risk	Clients who have defaulted in the past. Clients who have a suspicious background. Clients of Special Category Dormant Accounts

As per clause 2.2.4 and 2.2.5 of Guidelines on detecting suspicious transactions under Rule 7 (3) of the PML Rules,2005.

The following shall also be categorized as High Risk Clients/Transactions

Clause 2.2.4

- Countries subject to sanctions, embargoes or similar measures issued by, for example,

the United Nations ("UN"). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by a company because of the standing of the issuer and the nature of the measures.

- Countries identified by the Financial Action Task Force ("FATF") as non-co-operative countries and territories (NCCT) in the fight against money laundering or identified by credible sources as lacking appropriate money laundering laws and regulations
- Countries identified by credible sources as providing funding or support for terrorist activities.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

Clause 2.2.5

- Cash (and cash equivalent) intensive businesses.
- Money services businesses (remittance houses, money transfer agents and bank note traders.
- Casinos, betting and other gambling related activities, or
- businesses that while not normally cash intensive, generate substantial amounts of cash for certain transactions.
- Unregulated charities and other unregulated "not for profit" organisations (especially those operating on a "cross-border "basis)
- Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
- Clients that are politically exposed or "PEPs"

The above categorization shall be done initially at the time of opening of the Clients account and shall be reviewed on an ongoing basis depending of the trading pattern etc. of the clients.

Initial Risk categorization of all the clients would be done by the CCR Team depending on the financials details/ networth declarations and KYC declaration so of the clients given by the clients at time of account opening and regular updates received from the clients. Branch Officials shall inform CCR team in the event they feel the client belongs to the Medium or High Risk Category and specify reasons for the same. Risk categorization would also be modified depending on the trading patterns of the clients.

Monitoring Of Transactions

The monitoring for suspicious transaction should be done on following basis.

- The Origin of Funds
- The form in which funds were offered or withdrawn
- The destination of funds
- The form of instruction and authority
- The identity of the person undertaking the transaction

Special attention shall be paid to complex unusually large transactions/patterns have no economic purpose.

Threshold limits for review of various types of transaction and also shall be specified and reviewed by the Company from time to time with approval from.

The PMLA monitoring shall be carried out by the following Teams

Department	Broad Responsibility
CCR (account opening team)	Customer Acceptance Due diligence and Initial Risk Categorization
RMS Team	Monitoring of Trading pattern of clients and escalation of prima facie Suspicious Transaction
DP Team	Monitoring of DP Alerts and escalation of prima facie Suspicious Transaction
Principal Officer with Compliance Team	Review of prima facie Suspicious Transactions and reporting to FIU

The following alerts which are not system generated should also be raised to the principal officer if noted by any employee.

Sr. No.	Indicative Rules/Scenario
1	Customer did not open account after being informed about KYC requirements
2	Customer gives false identification documents or documents that appears to be counterfeited, altered or inaccurate.
3	Customer not staying at address provided during account opening
4	Customer uses complex legal structures or where it is difficult to identify the beneficial owner
5	Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences
6	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities.
7	Customer's name appears in any order passed by SEBI. SEBI has initiated an investigation and has restrained individuals/entities from buying, selling or dealing in the securities markets, either directly or indirectly, in any matter.
8	Match of customer details with persons reported in local media/open source for criminal offences
9	Match of customer details with persons reported in local media/open source for

	terrorism or terrorist financing related activities.
10	Customer did not complete transaction after queries such source of funds etc
11	Customer changes the information provided after more detailed information is requested
12	Customer provides information that seems minimal, possibly false or inconsistent.
13	Customer travels unexplained distances to conduct transactions
14	Customer makes inquiries or tries to convince staff to avoid reporting
15	Customer could not explain source of funds satisfactorily
16	Transaction is unnecessarily complex for its stated purpose.
17	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer
18	Transaction involving movement of which is inconsistent with the customer's business
19	Foreign remittance received by NPO not approved by FCRA
20	Where orders are being placed by an individual who holds a POA but is not a family member.
21	Complaint received from public for abuse of account for committing fraud etc.
22	Alert raised by agents about suspicion
23	Alert raised by other institutions, subsidiaries or business associates including cross-border referral
24	Transaction pattern same as that in orders passed by SEBI under the SEBI Act.

Suspicious transactions shall be regularly reported to the Principal Officer. There shall be continuity of dealing with the client & client shall not be informed of the Report. In some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents all such attempted transactions shall be reported in STRs, even if not completed by clients, irrespective of the amount of the transaction.

Freezing of funds, financial assets or economic resources or related services:

The Company shall ensure compliance with the procedures laid down in Order dated August 27, 2009 and Order dated March 14, 2109 under the Unlawful Activities (Prevention) Act, 1967.

Accordingly the Company shall review the updated list of list of individuals/ entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/ entities) as forwarded by SEBI from time to time and shall ensure the following:

1. Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the Schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of securities with them.
2. In the event, particulars of any of clients match the particulars of designated individuals/entities, the Company shall immediately, not later than 24 hours from the time of finding out such client, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such client on its books to the Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsctcr-mha@gov.in.
3. The Company shall also send the particulars of the communication mentioned in (2) above through post/fax and through e-mail (**sebi_uapa@sebi.gov.in)** to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND.
4. In case the aforementioned details of any of the customers match the particulars of designated individuals/entities **beyond doubt,** the Company should prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011- 23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsctcr-mha@gov.in.
5. The Company shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (2) above carried through or attempted, as per the prescribed format.
6. No prior notice should be given to the designated individuals/entities

Screening of Employees And Training on Prevention of Money Laundering

The Company shall have strict screening measures in place to ensure high standards when hiring employees

Training To Employees

The Company shall provide anti-money laundering training to all its new employees at the time of joining the organization and updates would be provided on periodic basis i.e. yearly basis to its all employees. The training shall review applicable money laundering laws and recent trends in money laundering activities as well as the Company's policies and procedures to combat money laundering, including how to recognize and report suspicious transactions.