



**POLICY AND PROCEDURE IN COMPLIANCE
WITH THE REQUIREMENTS OF
THE PREVENTION OF MONEY-
LAUNDERING ACT, 2002**

**ADOPTED BY
MONEYWISE FINVEST LIMITED**

Version: AML_2025-26_V.01

TABLE OF CONTENTS

S. No.	PARTICULARS	Page No.
1.	INTRODUCTION	3
2.	SCOPE AND APPLICABILITY	4
3.	APPOINTMENT OF OFFICERS FOR ENSURING COMPLIANCE WITH PROVISIONS OF PMLA	5
4.	POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING	5
4.1.	OBLIGATION TO ESTABLISH POLICIES AND PROCEDURES	5
4.2.	BROAD COVERAGE	7
5.	WRITTEN ANTI MONEY LAUNDERING PROCEDURES	7
5.1.	CLIENT ACCEPTANCE POLICY	10
5.2.	CLIENT IDENTIFICATION PROCEDURE	13
5.3.	RISK MANAGEMENT	16
5.4.	TRANSACTION MONITORING	18
5.4.1.	IDENTIFICATION / MONITORING OF THE SUSPICIOUS TRANSACTIONS	18
5.4.2.	SUSPICIOUS TRANSACTION MONITORING AND REPORTING	18
6.	RECORD MANAGEMENT	21
6.1.	RECORD KEEPING	21
6.2.	RETENTION OF RECORDS	22
7.	PROCEDURE FOR FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES	23
7.1.	LIST OF DESIGNATED INDIVIDUALS/ ENTITIES	24
7.2.	JURISDICTIONS THAT DO NOT OR INSUFFICIENTLY APPLY THE FATF RECOMMENDATIONS	26
7.3.	REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA	26
8.	PERSONNEL HIRING / RECRUITMENT AND TRAINING / INVESTOR EDUCATION	27
9.	INTERNAL CONTROL/AUDIT	28
10	POLICY APPROVAL & REVIEW	28

INTRODUCTION

The Prevention of Money Laundering Act, 2002 ("PMLA") and the Prevention of Money-Laundering Rules, 2005, as amended from time to time and notified by the Government of India, mandate every reporting entity to adhere to client account opening procedures, maintain records and report such transactions as prescribed therein to the relevant authorities. The PML Rules, inter alia, empower regulators to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by the regulator.

This policy stipulates the essential principles for combating Money Laundering (ML) and Terrorist Financing (TF) and provides detailed procedures and obligations to be followed and complied with by the company.

This policy shall also apply to the branches of company and its subsidiaries, if any, situated abroad, especially, in countries which do not apply or insufficiently apply the recommendations made by the Financial Action Task Force (FATF), to the extent local laws and regulations permit. When the local applicable laws and regulations prohibit implementation of these requirements, the same shall be brought to the notice of Regulators.

Regulators have from time to time issued circulars/directives with regard to Know Your Client (KYC), Client Due Diligence (CDD), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) specifying the minimum requirements. It is emphasized that the registered intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

1. Essential Principles for Compliance with PMLA Directives:

- i. The company policy is aligned with the PMLA directive as applicable to intermediaries registered under Section 12 of the SEBI Act. The policy provide relevant measures and procedures designed to assist registered intermediaries in preventing money laundering (ML) and terrorist financing (TF). In instances where there is a discrepancy between the Client Due Diligence (CDD) and Anti-Money Laundering (AML) standards stipulated by SEBI/ PMLA and those of the host country's regulators, it is imperative for the branches and overseas subsidiaries of registered intermediaries to adopt the more stringent of the two standards.

- ii. If the host country's regulation does not permit the proper implementation of AML/CFT measures in alignment with home country requirements, financial groups are obligated to apply suitable additional measures to manage the ML/TF risks. Furthermore, such instances must be reported to the regulator for appropriate action.

2. SCOPE AND APPLICABILITY

The provisions of PMLA and the Prevention of Money-Laundering PML Rules, 2005, as amended from time to time and notified by the Government of India requires every reporting entity to adhere to the client account opening procedures, maintenance records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

The PML Rules empowers Regulators to specify the information required to be maintained by the intermediaries and the procedure, manner and form in which it is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by the regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by regulator.

In accordance with the PMLA, violating the prohibitions on manipulative and deceptive devices, insider trading, or substantial acquisition of securities or control will be considered as scheduled offences under Schedule B of the PMLA. MONEYWISE FINVEST LIMITED, the company, is registered with SEBI to act as a Stock Broker; Depository Participant; Regulators have further issued Guidelines / Directions with regards to Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Intermediaries specifying the minimum requirements including comprehensive guidelines on Know Your Customer (KYC) norms, Client Due Diligence (CDD) and has advised all Intermediaries to ensure that a proper policy framework on KYC/CDD and AML/CFT measures be formulated and put in place with the approval of the Board of the intermediary.

Therefore, the company is required to comply & fulfill requirements as provided in the circulars/notifications/guidelines issued by regulatory authorities and any other circulars/notifications/guidelines as may be issued from time to time.

3. Appointment of officers for ensuring compliance with provisions of PMLA

3.1 Appointment of a Principal Officer: To ensure that the company properly discharges its legal obligations to report suspicious transactions to the authorities, the Company shall appoint a Principal Officer. In terms of Rule 2 (f) of the PML Rules, Principal Officer means an at the management level. The Principal Officer shall 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 and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU-IND.

3.2 Appointment of a Designated Director: The Company, in addition to Principal Officer shall also designate Managing Director or a Whole-Time Director and in the absence of same, any director of company as may be authorized by the Board of Directors; as a 'Designated Director' in terms of the PML Rules to ensure overall compliance with the obligations imposed under PML Rules. The Company shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

4. Policies and Procedures to Combat Money Laundering and Terrorist Financing

4.1. Obligation to establish policies and procedures

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing.

Group-Wide Compliance with PMLA Regulations:

1. Groups are required to implement comprehensive, group-wide policies to fulfill their obligations under the PMLA. The term "group" is defined in accordance with clause (cba) of sub-rule (1) of Rule 2 of the PML Rules/ clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961, as amended from time to time. "group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes, -(i) is required to be prepared under any law for

the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or (ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident;

2. Financial groups shall establish and enforce group-wide programmes to effectively address money laundering (ML) and terrorist financing (TF) across all branches and majority-owned subsidiaries. These programmes should include:
 - a. policies and procedures for sharing information required for Customer Due Diligence (CDD) and ML/TF risk management.
 - b. the provision at group-level compliance, audit, and/or AML/CFT functions of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes.

c. adequate safeguards on the confidentiality use of information exchanged, including safeguards to prevent tipping-off: The company will adhere to policy (including group-wide policy if any) and procedure for dealing with ML/TF in respect to sharing information, customer, account, and transaction information includes analysis of transactions or activities which appear unusual when necessary for AML/CFT purpose. However, this must be done without breaching confidentiality or the obligation to prevent tipping-off and complies with regulatory guidelines for conducting its businesses.

To be in compliance with above referred obligations, the senior management of company is fully committed to establishing appropriate internal policies & procedures and ensuring effectiveness and compliance with all relevant legal and regulatory requirements. The company shall:

4.1.1. issue policy for dealing with ML and TF reflecting the current statutory and regulatory requirements;

- 4.1.2. ensure that the content of this policy are understood by all staff members;
- 4.1.3. regularly review the policy and procedures on the prevention of ML and TF to ensure their effectiveness.
- 4.1.4. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
- 4.1.5. undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;
- 4.1.6. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and

- 4.1.7. develop staff members' awareness and vigilance to guard against ML and TF.

4.2. Broad coverage:

- 4.2.1. Communication of the group policy relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;
- 4.2.2. Client acceptance policy and client due diligence measures, including requirements for proper identification;
- 4.2.3. Maintenance of records;
- 4.2.4. Compliance with relevant statutory and regulatory requirements;
- 4.2.5. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
- 4.2.6. Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, 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; and,
- 4.2.7. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

5. Written Anti Money Laundering Procedures

The company is required to 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.

The following policy outlined below has been prepared in view of the above cited circular and guidelines.

CLIENT DUE DILIGENCE

Client Due Diligence means due diligence carried out on a client referred to in clause (ha) of sub section (1) of Section 2 of the PMLA using reliable and independent sources of identification. Here Client means, a person who is engaged in a financial transaction or activity with a reporting entity and

includes a person on whose behalf the person who engaged in the transaction or activity, is acting;

The CDD measures comprise the following:

- i. 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;
- ii. Identify the clients, verify their identity using reliable and independent sources of identification, and obtain information on the purpose and intended nature of the business relationship, where applicable. The company shall verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the company shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person. In case of a Trust, it will be ensure that trustees disclose their status at the time of commencement of an account based relationship;
- iii. The company shall identify the beneficial ownership & control by determining the individual(s) who ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted. The beneficial owner shall be determined as under:
 - a. where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation:- For the purpose of this sub-clause:-

- i). "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;
 - ii). "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;
- b. where the client is a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or

through one or more juridical person, has ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation:-For the purpose of this clause:- “Control” shall include the right to control the management or policy decision;

- c. where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent of the property or capital or profits of such association or body of individuals;
- d. Where no natural person is identified under clauses (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
- e. Where the client is a trust: Where the client is a trust, the company 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 beneficiaries with 10% 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;
- f. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies;
- g. Applicability for foreign investors: While dealing with foreign investors’, the identification of beneficial ownership of the client shall be determined as guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any;
- iv. The company shall 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. The company shall understand the ownership and control structure of the client;
- vi. The company shall conduct due diligence and scrutiny of client on an on-going basis, i.e. it shall perform on-going scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the company’s knowledge of the client, its business

and risk profile, taking into account, where necessary, the client's source of funds;

- vii. The company 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. The company shall take steps to periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.
- ix. The company shall take step to get register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the company has ended or the account has been closed, whichever is later
- x. Where company is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the company shall not pursue the CDD process, and shall instead file a STR with FIU-IND.
- xi. No transaction or account-based relationship shall be undertaken without following the CDD procedure

5.1. Client Acceptance Policy

The client acceptance policy of the company is designed with an aim to conduct a thorough evaluation of potential clients before onboarding on the basis of relevant parameters to identify and assess factors and the type of clients that are likely to pose a higher than average risk of ML or TF. By implementation of this policy, the company 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.

- 5.1.1.** The company shall not 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;
- 5.1.2.** The company shall classify clients into low, medium and high risk on the basis of risk perception (in terms of monitoring suspicious transactions) on the basis of 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. Clients of special category as listed below may be classified as high as such clients require higher degree of due diligence and regular update of Know Your Client (KYC)

profile;

5.1.3. The company shall undertake enhanced due diligence measures for Clients of Special Category (CSC) as prescribed by SEBI.

5.1.3.1. High Risk Clients which includes CSC are as provided below:

- a) Non - resident clients;
- b) High net-worth clients;
 - aa) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations;
 - bb) Companies having close family shareholdings or beneficial ownership;

c. Politically Exposed Persons (PEP): As per clause (db) of sub-rule (1) of rule 2 of the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, PEPs are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. The additional norms applicable to PEP as contained in the subsequent paragraph of the policy shall also be applied to the accounts of the family members or close relatives / associates of PEPs;

- d) **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 the company 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;

The company shall specifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

- e) **Non face to face clients:** Clients or subscribers who open accounts without visiting the branch/offices of the company or meeting the officials of the company. Video based customer

identification process is treated as face-to-face onboarding of Clients or subscribers

- f) Clients with dubious reputation as per public information available etc.;
- g) Client against whom Exchange/Regulator has issued show cause letter or has raised any query;
- h) Clients or subscribers which have been reported to FIU
- i) Once debarred Clients or subscribers after the expiry of debarment period
- j) Clients or subscribers who have undertaken dubious trades and due to this reason, the client(s) have been suspended by the company.
- k) Client creating high volumes in penny stock(s) and manipulated scrip(s).
- l) Defaulter(s) declared by stock exchange(s).

5.1.3.2. Medium Risk Clients:

- I. Clients under scanner of surveillance but no action taken but no queries/show cause notice letter received from Exchange/Regulator.
- II. Clients who were flagged in AML alerts and who were not able to provide sufficient justification for their transactions, resulting in logical closure without any suspicion being raised
- III. Clients against whom alerts has been raised by Exchange(s) for monitoring the activities.

5.1.3.3. Low Risk Clients:

All remaining Clients or subscribers have been kept under Low Risk Category

5.1.5. The company shall collect relevant documentation and other information in respect of different classes of clients depending on the perceived risk and having regard to the requirements for Client Due Diligence as provided in the PML Rules, Directives and Circulars issued by regulators from time to time.

5.1.6. In case the company is unable to apply appropriate CDD measures, the company shall ensure that such an account is not opened / not continue to do business with such persons. This shall apply in cases:

- 5.1.6.1. where it is not possible to ascertain the identity of the client,
- 5.1.6.2. or the information provided to the company is suspected to be non-genuine,
- 5.1.6.3. or there is perceived non-co-operation of the client in providing full and complete information.

5.1.7. The company shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The company shall be cautious to ensure that it does not return securities or money that

may be from suspicious trades. However, the company shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

5.1.8. The company shall permit clients to act behalf of another client / person / entity in instances which meets the following conditions:

5.1.8.1. Valid Authority letter / power of attorney / Board Resolution/ Court Order etc.

5.1.8.2. Relationship details of agent-client / Authorised Representative with the client entity on whose behalf the agent-clients shall be acting.

5.1.8.3. KYC details of agent – client / Authorised Representative.

5.1.8.4. Any other relevant documents.

5.1.9. The company shall put in place necessary checks and balances 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.

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

5.2. **Client identification procedure**

The company shall create/update its KYC policy clearly spelling out the client identification procedure (CIP) to be carried out at different stages i.e.

5.2.1. While establishing the client relationship,

- The company shall 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.
- The company shall obtain approval from Senior Management 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 approval from Senior Management to continue the business relationship.
- The company shall take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
- The client shall be identified by the company by using reliable sources including documents / information. The company shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended

nature of the relationship.

- It shall be ensured that information collected must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the company in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
- Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the senior management.
- Client(s) or subscriber(s) shall be registered as per Rules, Regulations, bye laws and circulars prescribed by the Regulatory Authorities from time to time.
- Prior to registration, Client(s) or subscriber(s) shall be properly identified by checking the furnished "Officially valid document" prescribed under PML Rule and Permanent Account Number "PAN" in original and obtaining copies thereof. PAN details of the client or subscriber shall be verified through the website provided by the Income Tax Authority. Client or subscriber where submits his Aadhaar number, ensure such client or subscriber to redact or blackout his Aadhaar number through appropriate means.

5.2.2. While carrying out transactions for the client or

- A continuous familiarity and follow-up shall be maintained with clients or subscribers, so that company is aware of the clients or subscriber on whose behalf it is dealing. Account opening application shall be rejected in case where the client or subscriber decline to cooperate during identity verification.
- Risk-based Approach shall be adopted. Customers of a higher risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. shall be applied "customer due diligence" measures on a risk sensitive basis through enhanced due diligence (EDD) process & through the type and amount of identification information and documents that are obtained.
- Further, low risk provisions will not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.
- Due Diligence for all Customers shall be carried out by identifying the beneficial ownership and control over securities account as prescribed by the Regulatory Authorities from time to time, 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. The identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted shall also be verified.
- when the company has doubts regarding the veracity or the adequacy of previously obtained client identification data.

5.2.3. *when the company has doubts regarding the veracity or the adequacy of previously obtained client identification data*

- *Where there is perceived non-cooperation of the client or subscriber in providing full and complete information, the Company shall cease to continue business with such a person(s)/ body corporate and file a suspicious activity report.*
- *The company shall conduct ongoing due diligence where it notices inconsistencies in the information provided.*
- *The company is committed to keeping its records up-to-date and accurate, and will ensure that any changes or updates to client and beneficial owner information are promptly incorporated into the relevant documents.*
- *There shall be no minimum threshold or exemption from obtaining the minimum information/ documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) for verification of the records of the identity of clients in respect of any category of clients.*
- *Any change which is inconsistent with the normal and expected activity of the client / subscriber shall lead to further ongoing due diligence processes and action as considered necessary.*
- *The company shall endeavor to identify the source of funds / contribution and ensure that the contribution is being done through the clients / subscriber's source of funds.*
- *The company shall provide reminders to clients for obtaining update of any such documents which were provided by the client at the time of initiation of client relationship as part of ongoing client due diligence for the purpose of updating the records within 30 days of such updation.* SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Based on these principles, the company shall develop internal directives tailored to their client interactions and legal obligations.
- *The company shall formulate and implement a Customer Identification Programme (CIP) in accordance with PML Rules as amended. This CIP will be included procedures and manner for maintaining records of transactions, methods and timelines for furnishing information, and verification processes for client identity. Additional requirements should be included to accurately determine client identities.*
- *Irrespective of the amount of investment made by the client no minimum threshold or exemption would be given by the company for obtaining minimum information/ documents from clients as per PML Rules and SEBI Circulars. Further, there are no exemptions or minimum thresholds for CDD measures.*

5.2.4. *The company may enlist the services of a third party to carry out identification and verification procedures for clients or subscriber, as well as to determine and verify the identity of beneficial owners. The company shall ensure that enlisted third-*

party entity is a regulated, supervised, or monitored for, and will have established measures in place to ensure compliance with Customer Due Diligence (CDD) and record-keeping requirements in accordance with the obligations set forth under the PML Act.

5.2.5. The use of third party for carrying out Client Due Diligence (CDD) by the company shall be subject to the conditions as specified below and shall be in accordance with PML Rules, regulations and circulars/ guidelines issued by regulators from time to time.

- The company shall immediately obtain necessary information of such client due diligence carried out by the third party;
- The company shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- The company shall ensure that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the regulatory requirements and obligations & Rules and Regulations made thereunder;
- The company shall ensure that third party is not based in a country or jurisdiction assessed as high risk;

5.3. Risk Management

5.3.1. Risk-based Approach

5.3.1.1. The company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk. The company shall monitor the implementation of the controls and enhance them if necessary.

5.3.1.2. The company shall categorise clients in higher or lower risk category depending on the circumstances after identifying and assessing the risks associated with a specific client such as the client's background, type of business relationship or transaction, product, service, or geographic location to determine the level of due diligence required. The company shall apply each of the client due diligence measures on a risk sensitive basis. The company shall adopt enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that company shall obtain will depend on the risk category of a particular client.

5.3.1.3. Further, low risk provisions shall not apply when there are

suspensions of ML/FT or when other factors give rise to a belief that the client does not in fact pose a low risk.

- 5.3.1.4.** The company shall examine, as far as reasonably possible, unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, reporting entities should be required to conduct enhanced due diligence measures, consistent with the risks identified.
- 5.3.1.5.** The company shall verify the identity of the client / subscriber through various modes/ methods of KYC as specified through circulars / guidelines issued by the regulators from time to time.
- 5.3.1.6.** The company shall examine the ownership and financial position; including clients / subscriber's source of funds commensurate with the assessed risk of client/subscriber and his/her profile.
- 5.3.1.7.** The overall responsibility /implementation and adherence of this shall lie with the Compliance, RMS & Surveillance Department of the company.
- 5.3.1.8.** The Concurrent/Internal auditors shall specifically check and verify the application of KYC/AML procedures and comments on the lapses observed in this regard. The reports and compliance in this regard shall also put up before the ODM committee / Audit Committee of the Board.

5.3.2. Risk Assessment

- 5.3.2.1.** 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.
- 5.3.2.2.** 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.

The company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The company shall ensure:

 - a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
 - b. Adoption of a risk based approach to manage and mitigate the risks

5.3.2.3. 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.

5.4. TRANSACTION MONITORING

5.4.1. Identification / Monitoring of the suspicious Transactions

5.4.1.1. The company shall have systems in place to identify and generate alerts for all complex unusually large transactions / patterns which appear to have no economic purpose. The company shall set an 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 relevant Authorities as and when required.

5.4.1.2. The company shall apply client due diligence measures to existing clients also on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

5.4.1.3. The company shall ensure a record of the transactions is preserved and maintained and that transactions of a suspicious nature or any other transactions notified under PMLA Act are reported FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the company

5.4.1.4. The compliance 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.

5.4.2. Suspicious Transaction Monitoring and Reporting

The company shall put in place systems to identify transactions on the basis of defined parameters and shall generate alerts for further analysis and reporting of suspicious transactions to FIU-IND. While determining suspicious transactions, the company shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

Here, "Suspicious transaction" as defined in the PML rules; means a

transaction including an attempted transaction, whether or not made in cash, which to a person acting in good faith

- (a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- (b) appears to be made in circumstances of unusual or unjustified complexity; or
- (c) appears to have no economic rationale or bona fide purpose; or
- (d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Explanation - Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

I. The company has identified a list of indicative circumstances to identify whether a particular transaction is suspicious or not depending upon the background, details of the transactions and other facts and circumstances:

- i. Clients whose identity verification seems difficult or clients that appear not to cooperate;
- ii. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
- iii. Clients based in high risk jurisdictions;
- iv. Substantial increases in business without apparent cause;
- v. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- vi. Attempted transfer of investment proceeds to apparently unrelated third parties;
- vii. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.
- viii. *Prospective clients or subscribers who do not open an account after being informed about the KYC requirements of in-person meeting, verification of original OVD or who provide minimal, false or inconsistent information.*
- ix. *Clients or subscribers who provide false identification documents or documents that appears to be forged or inaccurate.*
- x. *Clients or subscribers who use complex legal structures to hide the identity of the actual beneficial owner.*
- xi. *Clients or subscribers whose details match those reported in local media or open sources for criminal offenses or terrorism.*
- xii. *Clients or subscribers who cannot satisfactorily explain the source of their funds, or whose transactions involve movement of funds that is inconsistent with their business.*

- xiii. Transactions that have no economic rationale, or whose frequency, amount, or stated reason does not make sense for the particular client.*
- xiv. Complaints received from the public about account abuse for committing fraud or other illicit activities.*
- xv. Clients or subscribers who have been the subject of an inquiry by any law enforcement agency relating to criminal offenses.*
- xvi. Clients or subscribers who make inquiries or attempt to convince staff to avoid reporting any of the above red flags.*

- II.** Any suspicious transaction shall be immediately notified to the Designated/Principal Officer. The notification shall be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion.
- III.** However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion.
- IV.** 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.
- V.** The Designated/ Principal 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.
- VI.** In cases where transactions are abandoned or aborted by clients on being asked to give some details or to provide documents; the company shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.
- VII.** The company shall ensure that clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards and which have been categorized as 'CSC' by regulators, are subject to appropriate counter measures. These measures shall include a 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.
- VIII.** All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as d-mat account, security account maintained by the company. Record of all transactions where any forgery of a valuable security has taken place.
- IX.** The company shall review transactional alerts received from depositories, stock exchanges, and regulatory agencies from AML/CFT

perspective.

6. Record Management

Information to be maintained

The company is required to maintain and preserve the following information in respect of transactions referred to in PML Rules:

- i. the nature of the transactions;
- ii. the amount of the transaction and the currency in which it is denominated;
- iii. the date on which the transaction was conducted; and
- iv. the parties to the transaction.

6.1. RECORD KEEPING

6.1.1. The company shall ensure compliance with the record keeping requirements as directed by PMLA, Rules and Regulations made thereunder as well as other relevant legislation, Rules, Regulations, Byelaws and Circulars.

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

6.1.3. It should be noted that in case of any suspected laundered money or terrorist property, the abovementioned records may be needed by, the competent investigating authorities to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, the company shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

- i. the beneficial owner of the account;
- ii. the volume of the funds flowing through the account; and
- iii. for selected transactions:
 - a. the origin of the funds
 - b. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
 - c. the identity of the person undertaking the transaction;
 - d. the destination of the funds;
 - e. the form of instruction and authority.

6.1.4. The company shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, it shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may

exceed those required under the relevant Acts, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

6.1.5. The company shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under PML Rules as mentioned below:

6.1.5.1.

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

6.1.5.3. For the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered by the company.

6.1.5.4. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by the company.

6.1.5.5. 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;

6.1.6. Where the company does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the company shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under rules 3 and 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

6.2. RETENTION OF RECORDS

6.2.1. 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 PML Rules shall be maintained and

preserved for a period of five years from the date of transactions between the client and company.

6.2.2. The company shall formulate and implement the CIP containing the requirements as laid down in the PML Rules and such other additional requirements that it considers appropriate. 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.

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

6.2.4. The company shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under PML Rules, for a period of five years from the date of the transaction between the client and the company.

7. Procedure for freezing of funds, financial assets or economic resources or related services

The company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, company do not have any accounts in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

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

1. The Ministry of Finance, Government of India, has issued an order dated January 30, 2023, detailing the procedure for implementing Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act). This order, accessible via the provided link, must be strictly followed.

2. As per Section 12A of the WMD Act, the Central Government is authorized to:

a. Freeze, seize, or attach funds, financial assets, or economic resources owned, controlled, or derived from prohibited activities related to weapons of mass destruction.

b. Prohibit the provision of funds, financial assets, or economic resources for the benefit of individuals or entities involved in prohibited activities under the WMD Act.

3. Registered intermediaries are obligated to adhere to the procedure outlined in the government order.

4. Key Responsibilities of Registered Intermediaries:

a. Maintain and promptly update a Designated List of individuals/entities.

b. Verify if transaction parties match the Designated List and report any matches to the Central Nodal Officer (CNO) immediately.

c. Conduct checks on new client relationships and periodically verify if clients match the Designated List, reporting any matches to the CNO promptly.

d. Notify the Nodal Officer of SEBI of relevant communications to the CNO.

e. Take immediate action to prevent designated individuals/entities from conducting financial transactions

f. File Suspicious Transaction Reports (STR) with the Financial Intelligence Unit-India (FIU-IND) for transactions involving designated individuals/entities.

5. Upon receipt of information, the CNO will verify the identified individuals/entities against the Designated List. If confirmed, an order to freeze assets will be issued.

6. Reporting entities must also comply with exemption provisions and address inadvertent freezing of accounts as applicable.

7.1. List of Designated Individuals/ Entities

7.1.1. The company shall take note of lists of individuals/entities communicated by Regulators from time to time; which are designated as "Terrorists" by the Ministry of Home Affairs in pursuance of Section 35(1) of UAPA 1967.

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

7.1.3. An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <https://press.un.org/en/content/press-release>. The details of the

lists are as under:

- 7.1.3.1. The “ISIL (Da’esh) & Al-Qaida Sanctions List”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: <https://www.un.org/securitycouncil/sanctions/1267/press-releases>.
- 7.1.3.2. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.
- 7.1.4. The company shall ensure that accounts are not opened in the name of anyone whose name appears in said list. The company shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.
- 7.1.5. The company shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them. The company shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.
- 7.1.6. The company shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.
- 7.1.7. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.
- 7.1.8. The company shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT, as provided on the website of Government of India, Ministry of Home Affairs; where the account is held and to SEBI and FIU-IND. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, “G” Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

7.2. Jurisdictions that do not or insufficiently apply the FATF Recommendations

- The company shall put in place additional / increased monitoring of clients / transactions emanating from jurisdictions with strategic deficiencies in their regimes to counter money laundering, terrorist financing and proliferation of financing risks as per public statements released by FATF Secretariat & circulated by Regulators from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations.
- The company shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements while entering / having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

7.3. Reporting to Financial Intelligence Unit-India

7.3.1. In terms of the PML Rules, the company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND). While reporting cash and suspicious transactions, the company shall adhere to the following:

7.3.1.1. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

7.3.1.2. The Non-Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month.

7.3.1.3. The Principal Officer will be responsible for timely submission of STR and NTR to FIU-IND;

7.3.1.4. Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND.

7.3.1.5. No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported.

7.3.1.6. The company, including its Directors, officers, and all employees, shall ensure that the maintenance of records and the furnishing of information to the Director remain confidential.

7.3.1.7. This confidentiality requirement does not prohibit the sharing of information required under the “policies by groups” of the PML Rules. Specifically, any analysis of transactions and activities that appear unusual can be shared, provided such analysis has been conducted.-profit organization” means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

7.3.2. The company shall not put any restrictions on operations in the accounts where an STR has been made. The company and its directors, officers and employees (permanent and temporary) are prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

7.3.3. The company shall, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified PMLA Act, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime;

Wherein "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

Confidentiality requirement does not inhibit information sharing among entities in the group.

8. PERSONNEL HIRING / RECRUITMENT AND TRAINING / INVESTOR EDUCATION

Personnel Hiring / Recruitment:

The company shall have adequate screening procedures in place to ensure high standards when hiring & recruitment of relevant personnel.

The Company shall identify the key positions within organization structures having regard to the risk of money laundering and terrorist financing and the size of business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

Training:

The company shall have an ongoing training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients as it is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

Investor Education

The company shall prepare literature/ pamphlets etc. to educate & sensitize the clients with regards to requirements emanating from PMLA framework and the objectives of the AML/CFT programme, which may require the company to seek certain additional information from clients which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc.

9. Internal Control/Audit:

The Company shall get its procedures and processes to monitor ML activity; periodically audited to verify compliance with the extant policies, procedures and controls relating to the prevention of ML and TF.

The company shall place suggestions / comments/ notes of auditor with regards to robustness of the internal policies and processes along with steps taken to strengthen the policy and implementation aspects before the ODM committee/ Audit Committee / Board of company.

10. Policy Approval & Review:

The policy shall be approved by the board the company and shall be periodically reviewed and updated as per requirement and on the basis of amendments in relevant Rules, Regulations, Byelaws and Circulars as issued by regulatory authorities. Further, policy shall be reviewed at least once in a year by the Board of company.

This Policy last reviewed & approved on 22th January 2026.