PMLA POLICY FOR CLIENT ACCEPTANCE

Effective Date: 09.06.2025 | **Prepared by:** Subhra Simantinee | **Approved By:** Board of Directors | Version: 2.0

1. OBJECTIVE AND SCOPE OF POLICY

This policy establishes a comprehensive internal mechanism to prevent Skywards Investec Private Limited ("the Company") from being used, intentionally or unintentionally, as a channel for Money Laundering (ML) or Terrorist Financing (TF).

This policy is designed in strict compliance with:

- The Prevention of Money Laundering Act, 2002 (PMLA).
- The Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time.
- SEBI Master Circular SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06, 2024.

2. SCOPE OF APPLICABILITY

This policy applies globally to all operations, business units, departments, branches, and majority-owned subsidiaries of the Company (if any).

Global Group Mandate: If the Company operates branches or overseas subsidiaries situated abroad, this policy applies to them to the extent local laws permit. If there is a variance between SEBI standards and host country regulations, the more stringent of the two must be adopted. If host country laws prohibit proper implementation of these AML/CFT measures, the matter must be formally brought to the notice of SEBI.

3. STATUTORY DESIGNATION OF COMPLIANCE OFFICERS

To ensure effective implementation and seamless regulatory reporting, the Board of Directors has designated the following senior-level officials:

3.1 Designated Director

- **Name / Status:** Chandrakiran Bogadi, Director and CEO of the Company**.**

- **Statutory Role:** In terms of Rule 2(ba) of the PML Rules, the Designated Director is appointed to ensure overall compliance with the obligations imposed under Chapter IV of the Act and Rules.

- **Regulatory Liability:** In terms of Section 13(2) of the PMLA, the Director, FIU-IND can levy monetary penalties or take appropriate legal actions directly against the Designated Director for any compliance failures by the intermediary.

- **Communication:** The details of the Designated Director shall be communicated to the Office of the Director, FIU-IND.

3.2 Principal Officer/Compliance Officer

- **Designee:** Mrs. Subhra Simantinee

- **Statutory Role:** In terms of Rule 2(f) of the PML Rules, the Principal Officer must be a key official at the **management level**. She acts as the central reference point for the identification, assessment, and onward reporting of suspicious or cash transactions.

- **Reporting Lines:** The Principal Officer shall have direct access to, and report to, the senior management at the next reporting level or the Board of Directors.

- **Communication:** Name, designation, and address changes of the Principal Officer must be promptly intimated to the Director-FIU-IND.

4. CORE PRINCIPLES OF THE CLIENT ACCEPTANCE POLICY (CAP)

The Company shall enforce the following safeguards during client onboarding and relationship maintenance:

- **Strict Prohibition of Anonymity:** No account shall be opened or kept in an anonymous, fictitious, or "benami" name, or on behalf of persons whose identity cannot be verified.

- **CDD Finality & Account Refusal:** No account shall be opened or maintained where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures. This includes cases of non-cooperation, non-genuine information, or inability to verify identity. If an existing relationship exhibits these issues, the account must be evaluated for closure after due notice, and a Suspicious Transaction Report (STR) must be filed.

- **Client Authority Verification:** Clear rules must govern circumstances where a client acts on behalf of another entity. The Company shall establish account operation methods, transaction limits, and verify the legal authority (such as Power of Attorney or Board Resolutions) of the agent.

- **Criminal Background Checks:** Necessary checks and balances must ensure that the identity of the client does not match any person with a known criminal background or who is banned/sanctioned worldwide by civil or criminal enforcement agencies.

5. CUSTOMER DUE DILIGENCE (CDD) BREAKDOWN

No transaction or account-based relationship shall be commenced without executing the full CDD procedure using reliable, independent sources.

5.1 Client Identification & Verification

- **Source Verification:** The identity of the client, the purpose, and the intended nature of the business relationship must be verified using reliable independent source documents, data, or information.

- **Trust Status Disclosure:** In the case of a Trust, the Company must ensure that trustees explicitly disclose their status at the time of commencement of the account-based relationship.
- **In-Person Verification (IPV):** Physical IPV or approved digital onboarding frameworks (such as SEBI-compliant Video-Based Customer Identification Processes) are mandatory to establish identity.

5.2 Strict Identification Thresholds for Beneficial Ownership (BO)

Beneficial Owners (natural persons who ultimately own, control, or influence a client) must be identified using the following revised regulatory thresholds:

Juridical Person / Entity Type	**Beneficial Ownership (BO) Threshold Parameter**
Company	Natural person(s) holding a controlling ownership interest of more than 10% of shares, capital, or profits. ("Control" includes the right to appoint a majority of directors or control management/policy decisions).
Partnership Firm	Natural person(s) holding ownership of / entitlement to **more than 10%** of capital or profits.
Unincorporated Association / Body of Individuals	Natural person(s) holding ownership of / entitlement to **more than 15%** of the property, capital, or profits.
Trust	Identification of the author, trustee, settlor, protector, beneficiaries with **10% or more interest**, or any natural person exercising ultimate effective control.
Senior Managing Official	If no natural person is identified under Companies, Partnerships, or Associations, the BO is the natural person holding the position of Senior Managing Official.

Exemption Note: Identification of individual shareholders/BOs is **not** required if the client is an entity listed on an Indian stock exchange, or listed in a notified foreign jurisdiction, or is a majority-owned subsidiary of such a listed entity.

Monitoring Governance: Compliance with BO identification will be monitored through half-yearly internal audits, with findings reviewed directly by the Board of Directors.

5.3 Ongoing Due Diligence, Updating, & Tipping-Off

- **Periodic Updating:** All client and BO documentation collected under CDD must be periodically updated and kept relevant, with strict frequency enforced for high-risk clients.
- **Re-verification Triggers:** CDD must be completely revisited whenever there are suspicions of ML/TF or doubts regarding the adequacy or veracity of previously obtained data.

- **DARPAN Portal Registration:** In the case of a Client being a **Non-Profit Organisation (NPO)**, the Company must register the client's details on the **DARPAN Portal of NITI Aayog**. These registration records must be preserved for **five years** after the relationship ends or the account is closed, whichever is later.
- **CDD vs. Tipping-Off:** If the Company suspects a transaction relates to ML/TF and reasonably believes that performing the CDD process will tip-off the client, **the Company shall halt the CDD process and immediately file an STR with FIU-IND**.

5.4 Reliance on Third Parties for CDD

The Company may rely on a regulated, supervised, or monitored third party to carry out client identification, verification, and BO determination only if:

I. Necessary information regarding CDD is obtained from the third party **immediately**.
II. The Company ensures identification data is made available by the third party upon request **without delay**.
III. The third party is **not** based in a high-risk country.
IV. The Company remains **ultimately responsible** for CDD and enhanced due diligence (EDD) measures.

6. RISK-BASED APPROACH (RBA) FRAMEWORK

The Company utilizes a formal Risk-Based Approach to categorize clients into Low, Medium, and High-risk segments based on specific parameters such as client location, nature of business, trading turnover, and payment methods.

6.1 No Exemptions / Threshold Immunity

There is no minimum investment threshold or category-wise exemption available for carrying out CDD measures. Every single client undergoes formal risk assessment and baseline verification.

6.2 Categories of Special Clients (CSC) & High-Risk Profiles

Clients categorized under the following brackets must be subject to **Enhanced Due Diligence (EDD)**, regular updates, and stricter monitoring:

- Non-resident clients and High Net-worth Individuals (HNIs).
- Trusts, Charities, NGOs, and organizations receiving donations.
- Companies having close family shareholdings or beneficial ownership.
- **Politically Exposed Persons (PEPs):** Individuals entrusted with prominent public functions, including their family members, close relatives, and associates.
- Non-face-to-face clients (excluding standardized video-based onboarding).
- Clients with a dubious reputation based on publicly available information.
- Corporate clients undergoing a structural Change in Dominant Promoter / Control (e.g., transfer of control or major transfers of Equity / Compulsorily Convertible Debentures).

6.3 Specific Mandates for High-Risk Countries

When dealing with clients or transactions originating from, situated in, or routed through high-risk countries or geographic areas (identified via public records or **FATF Statements** as lacking effective AML/CFT measures):

- The Company shall independently access and evaluate public risk vectors.
- **Proportionate Countermeasures / EDD** must be applied, including enhanced transaction scrutiny, systematic financial reporting, and strict limitations on expanding business relationships.
- Low-risk simplified provisions are strictly inapplicable if there is an ML/TF suspicion or any factor indicating a non-low risk profile.

6.4 Risk Assessment for New Products & Technologies

Prior to launching or deploying any new products, business practices, delivery mechanisms, or developing technologies (such as algorithmic trading tools or digital onboarding features), the Company **must carry out a formal ML/TF risk assessment** and adopt a risk-based approach to mitigate identified threats.

7. TRANS-ACTUAL MONITORING AND SUSPICIOUS TRANSACTION REPORTING (STR)

7.1 Transaction Monitoring Mandates

- **Baseline Activity Understanding:** The Compliance Department must maintain a clear understanding of the normal activity of each client to quickly recognize deviations or anomalies.
- **Complex Patterns:** Special attention must be given to all complex, unusually large transactions or patterns that appear to have no apparent economic or lawful purpose. Internal threshold limits must be set for client accounts.
- **Written Findings:** The background, including documents, office records, and clarifications sought for unusual transactions, **must be examined and recorded in writing**. These findings must be preserved and made available to internal/external auditors, SEBI, stock exchanges, and FIU-IND during inspections.

7.2 Recognition of Suspicious Transactions

Suspicious transactions (attempted or executed) include those that give rise to a reasonable ground of suspicion that they involve proceeds of crime, regardless of the transaction amount or any predicate offence thresholds. Indicators include:

- Identity verification is difficult, or the client is non-cooperative.
- Asset management funds have an unclear source, inconsistent with the client's standing.
- Unexplained substantial increases in business volumes or large cash/overseas routing.
- **Attempted or Aborted Trades:** If a client abandons or aborts a transaction upon being requested to provide documents or background details, **the attempted transaction must be reported in an STR to FIU-IND, irrespective of its value**.

7.3 STR Governance & Non-Interruption Rules

- **Continuity of Account Operations:** When an internal suspicion report is made to the Principal Officer, **the client must not be informed, and account operations must continue normally** to avoid tipping off. No operational restrictions or freezes shall be placed on the

account unless explicit statutory instructions or freezing orders are received from the authorities.

- **Tipping-Off Prohibition:** Directors, officers, and employees (permanent and temporary) are strictly prohibited from disclosing or tipping off the client or any third party that an STR or related analysis is being compiled or reported to FIU-IND.

8. RECORD KEEPING, RETENTION, AND DATA MANAGEMENT

The Company's internal record-preservation mechanism ensures quick data retrieval and satisfies strict statutory timelines:

8.1 Information to be Maintained

The Company shall capture and retain the following audit-trail parameters for all transactions:

- The nature, amount, and currency denomination of the transaction.
- The exact date of execution and identification of all parties involved.
- The beneficial owner of the account and the volume of funds moving through it.
- For selected entries: the origin of funds, destination of funds, the form of instruction/authority, and the specific instrument type (cheques, demand drafts, etc.).

8.2 Strict Record Retention Matrix

The corporate policy is updated to match the regulatory standard, replacing previous 8-year references with the statutory **PMLA 5-year retention architecture**:

RECORD RETENTION MATRIX	
Record / Information Type	**Statutory Retention Period**
Transactions prescribed under Rule 3 (Cash, Connected, Forged Currency)	5 Years from the exact date of the transaction.
Client KYC & Identity Evidence Records (Identity data, account files, etc.)	5 Years after the relationship has ended or closed.
Attempted or Executed Transaction Information Reported to FIU-IND	5 Years from the date of transaction
Ongoing Investigations / Active STRs	Retained indefinitely until confirmed closed.

8.3 Rule 3 Value Thresholds

Proper records must be systematically maintained for the following transaction types:

- All cash transactions valued at **more than ₹10 Lakhs** or its foreign currency equivalent.
- Series of integrally connected cash transactions valued below ₹10 Lakhs individually, but which **aggregate above ₹10 Lakhs within a single calendar month**.

- All cash transactions where forged or counterfeit currency notes or bank notes have been used.
- All suspicious transactions (cash or non-cash), including credits/debits into or from any non-monetary account (such as demat or security accounts).

9. SANCTION SCREENING AND ASSET FREEZING PROCEDURES

9.1 Terrorist Links & UAPA Section 51A Implementation

- Sanction Lists Monitoring: The Company must continuously scan its existing databases and ensure no accounts are opened or held by individuals/entities listed on the United Nations Security Council (UNSC) Sanctions Lists (including the Al-Qaida & ISIL Sanctions List and the DPRK Sanctions List) or designated by the Ministry of Home Affairs (MHA) under Section 35(1) of the UAPA.
- Name Screening Tools: The Company must maintain updated electronic lists and leverage latest technological tools for name screening.
- Reporting Matches: Any match with UAPA lists must be immediately reported to the Central Nodal Officer for UAPA at MHA, the Nodal Officers of the State/UT, SEBI, and FIU-IND via email (sebi_uapa@sebi.gov.in), and an STR must be filed.

9.2 Weapons of Mass Destruction (WMD) Act Section 12A Implementation

In terms of Section 12A of the WMD Act, 2005, and the Ministry of Finance Order dated January 30, 2023, the Company shall enforce the following strict directions:

- **Designated List Checks:** Maintain and update the WMD "Designated List" without delay. Run automated checks at onboarding and periodically against this list.
- **Match Actions:** If an identity match is found, the Company **shall not carry out the transaction** and must immediately freeze/prevent the entity from conducting financial transactions. Full particulars of the assets, bank accounts, or stocks must be informed to the Central Nodal Officer (Director, FIU-IND) and the Nodal Officer of SEBI within post/email channels without delay.
- **STR Obligation:** A formal STR must be filed covering all transactions executed or attempted through such flagged accounts.

10. REGULATORY REPORTING SCHEDULE TO FIU-INDIA

All notifications to the Financial Intelligence Unit-India (FIU-IND) must be handled by the Principal Officer using the official FINnet 2.0 portal:

- Cash Transaction Reports (CTR): Must be submitted to FIU-IND by the 15th day of the succeeding month.
- Non-Profit Organization Transaction Reports (NTR): Must be submitted to FIU-IND by the 15th day of the succeeding month.
- Suspicious Transaction Reports (STR): Must be submitted within 7 days of arriving at a conclusion that any transaction or series of connected transactions are of a suspicious nature. The Principal Officer must formally record the reasons for treating a transaction as suspicious.

- No NIL Reporting: No "NIL" reporting is required if there are no cash, suspicious, or NPO transactions executed during a month.

- Confidentiality: The fact that information is being compiled or shared within the group for analysis must remain strictly confidential.

11. GOVERNANCE, TRAINING, AND HR EVALUATION

11.1 Hiring Framework
The Company shall implement adequate screening procedures to ensure high standards when hiring employees. Key risk-sensitive roles (frontline onboarding, compliance, back office, and risk management) must be evaluated to ensure personnel are competent to handle PMLA duties.

11.2 Ongoing Training Programs
The Compliance Department shall run periodic training initiatives tailored to frontline staff, back-office executives, and risk analysts. This training covers:

- The rationale behind SEBI AML/CFT Directives.
- Recognition of complex transaction deviations.
- Interdisciplinary Integration: Bridging the gap between AML/KYC requirements and Credit Risk Analysis. Employees will be trained to use credit risk management frameworks to identify operational and compliance risks within client loan and processing life cycles.

11.3 Investor Education
To handle inquiries regarding requests for sensitive personal information (such as income tax returns, net worth certificates, or bank records), the Company shall publish pamphlets and educational literature to sensitize clients on global AML/CFT safety objectives.

12. REPEAL AND SAVINGS
This revised policy stands effective immediately upon approval by the Board of Directors. All prior internal compliance guidelines or policy sections drawn from older circulars are superseded. Any actions taken under past versions shall be deemed to have been executed under the corresponding sections of this Master Circular-compliant policy.

13. INTERNAL GOVERNANCE AND OVERSIGHT
The Compliance Officer, Subhra Simantinee, leads the internal governance framework. Her responsibilities include:

- **Liaison Duties:** Serving as the principal point of contact for NSE, BSE, NCL, CDSL, and NSDL.
- **Audit Management:** Leading exchange inspections and regulatory audits, ensuring the prompt resolution of any observations or deficiencies.
- **Statutory Filings:** Supervising the timely submission of statutory disclosures and the maintenance of the Internal Compliance Framework.
- **Strategic Advisory:** Advising the Board on the impact of regulatory developments on the company's risk management and growth initiatives.

14. REPORTING OBLIGATIONS

The Principal Officer is responsible for filing the following with FIU-IND:

- **Suspicious Transaction Reports (STR):** To be filed within 7 working days of arriving at a conclusion that a transaction (attempted or executed) is suspicious.
- **Cash Transaction Reports (CTR):** For all cash transactions exceeding the prescribed thresholds.

15. POLICY REVIEW AND TRAINING

- **Regulatory Alignment:** This policy is subject to periodic review to ensure synchronization with updated SEBI and NSE circulars.

- **Interdisciplinary Training:** The Compliance Department shall conduct training sessions that bridge the gap between AML/KYC requirements and Credit Risk Analysis. Utilizing the Compliance Officer's expertise in PhD-level Credit Risk Management, staff shall be trained to identify operational risks within the loan processing and client acceptance lifecycles to ensure sustainable and compliant growth.

Policy Endorsement & Sign-Off

For Skywards Investec Private Limited
Reviewed by: Mrs. Subhra Simantinee (Principal Officer)
Adopted by: Board of Directors