

-MONEY LAUNDERING (AML) & PMLA POLICY

1. Introduction & Objectives

As a registered market intermediary, the company is committed to preventing the Indian capital markets from being used for money laundering or terrorist financing.

- **Regulatory Backbone:** This policy is framed in compliance with the **Prevention of Money Laundering Act, 2002 (PMLA)**, PML Rules, 2005, and relevant SEBI AML Guidelines.
 - **Key Targets:**
 1. Establish robust Customer Due Diligence (CDD) systems.
 2. Implement an ongoing transaction monitoring system to flag suspicious patterns.
 3. Report mandatory financial and suspicious transactions to **FIU-IND**.
 4. Ensure records are safely maintained for required statutory durations.
-

2. Appointment of Compliance Officials

To oversee implementation, the Board of Directors designates senior officials to independent oversight roles:

- **Principal Officer:** Responsible for overall monitoring, evaluating suspicious flags, and filing reports to FIU-IND.
 - *Name / Designation:* SUNNY AGARWAL/ COMPLIANCE OFFICER
 - **Designated Director:** Ensures organizational compliance with the statutory provisions of the PMLA.
 - *Name / Designation:* SURESH KUAMR JALAN/ PROPRIETOR
-

3. Customer Due Diligence (CDD) Measures

The firm will strictly execute CDD protocols before enabling any account for active trading:

3.1 Verification and Identification

- **PAN Verification:** Every PAN card must be instantly verified against the Income Tax database.
- **Officially Valid Documents (OVDs):** Identity and address must be substantiated via dynamic e-KYC or physical verification of OVDs (Aadhaar, Passport, Driving License).

- **Financial Auditing:** Clients intending to trade in Derivatives (F&O, Currency, Commodity) must submit active bank statements, ITR acknowledgments, or net-worth certificates.

3.2 Ultimate Beneficial Owner (UBO) Screening

For non-individual entities (Companies, Partnerships, Trusts), the corporate compliance desk must run cross-checks to isolate natural persons exercising control (holding >10% controlling interest in corporations or >15% in partnerships/trusts).

4. Client Risk Categorization (CRC)

Clients are bifurcated into risk tiers based on financial background, geographic origin, and business channels:

[Low Risk]	-> Standard Retail/Salaried; basic monitoring.
[Medium Risk]	-> High Net-worth Individuals (HNIs); quarterly transaction checks.
[High Risk]	-> PEPs, FPIs, Unregistered NGOs; Enhanced Due Diligence (EDD).

- **Enhanced Due Diligence (EDD):** High-risk clients and Clients of Special Category (CSC) must face senior management approval prior to account activation. The source of wealth/funds must be thoroughly documented.

5. Transaction Monitoring Framework

The risk management system (RMS) will deploy automated triggers to flag irregular trading and payment patterns:

- **Disproportionate Volumes:** Transactions that appear highly inconsistent with the client's declared financial capacity or net worth.
- **Third-Party Fund Rejections:** Automated rejection of funds transferred via bank accounts or depository participants not registered under the client's matching credentials.
- **Off-Market Demat Movements:** High-volume off-market transfers inside a single Demat account without explicit, logical commercial basis.
- **Sudden Dormant Reactivation:** High-value volumes abruptly appearing in accounts that were inactive for a prolonged period.

6. Reporting Obligations to FIU-IND

The Principal Officer shall securely transmit reports to the Financial Intelligence Unit - India via the FINNET portal:

Suspicious Transaction Report (STR): Filed within **7 working days** of the Principal Officer determining that a transaction (or attempted transaction) involves laundered money or illegal assets, regardless of the transaction amount.

7. Retention of Records

All essential regulatory records must be preserved for **5 years** from the date of the cessation of the relationship or transaction date, whichever is longer:

- Client KYC portfolios, address/ID copies, and verification files.
 - Ledger accounts, contract notes, and trade logs.
 - Internal documentations concerning flagged alerts, internal analysis, and filed STRs.
-

8. Staff Training & Policy Review

- **Employee Screening:** HR must perform reference and background vetting before hiring personnel into compliance, RMS, and account opening desks.
 - **Periodic Audit:** The Internal Audit/Compliance team must review the effectiveness of the AML framework annually.
 - **Board Review:** This policy must be updated to align with any sudden modifications, amendments, or circulars released by SEBI, RBI, or the Stock Exchanges.
-

