PARDIWALA SECURITIES PVT LTD

ANTI-MONEY LAUNDERING (AML),
COUNTERING THE FINANCING OF TERRORISM (CFT)
AND COUNTERING PROLIFERATION FINANCING (CPF) POLICY

1. Policy Statement

Pardiwala Securities Pvt Ltd is committed to preventing the use of its securities-market services for money laundering, terrorist financing, proliferation financing, fraud, tax evasion, sanctions evasion and other unlawful activities. The Company shall maintain a risk-based AML/CFT/CPF framework consistent with applicable Indian law, SEBI requirements, FIU-IND requirements and other directions applicable to its business.

This policy applies to the Company's directors, employees, authorised persons/intermediaries, contractors and other persons acting on behalf of the Company, and to all clients and prospective clients to the extent relevant to the Company's services.

2. Regulatory Framework

The policy shall be read with the Prevention of Money Laundering Act, 2002 ("PMLA"), the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 ("PML Rules"), SEBI's applicable AML/CFT master circulars and amendments, FIU-IND directions and guidance, SEBI KYC requirements, applicable sanctions/proscription requirements, and other laws and regulations applicable to the Company.

The Company shall update this policy whenever applicable law, regulation, circular, notification or guidance changes. Where there is a conflict, the applicable law/regulatory requirement shall prevail.

3. Objectives

- Know and identify every client and, where applicable, the person acting on behalf of the client and the beneficial owner.
- Prevent anonymous, fictitious, benami and otherwise unacceptable relationships.
- Apply a documented risk-based approach to customer acceptance, enhanced due diligence and ongoing monitoring.
- Detect and investigate unusual, complex, unusually large or economically unexplained transactions and patterns.
- Identify and report suspicious transactions and other prescribed transactions to FIU-IND within the applicable timelines.
- Maintain records and confidentiality as required by law.
- Prevent tipping-off and protect the integrity of investigations and regulatory reporting.
- Provide regular AML/CFT/CPF training and maintain appropriate independent testing and internal controls.

4. Governance and Responsibilities

4.1 Board of Directors

- Approve this policy and significant amendments.
- Provide adequate resources, authority and oversight for AML/CFT/CPF compliance.
- Review material AML/CFT/CPF risks, significant compliance issues and remediation status.

4.2 Designated Director

The Company shall designate a Designated Director in accordance with the PMLA/PML Rules. The Designated Director shall have overall responsibility for ensuring compliance with applicable Chapter IV obligations and shall oversee the adequacy of systems, controls, risk assessment, record keeping, CDD, transaction monitoring and reporting.

4.3 Principal Officer

The Company shall appoint a management-level Principal Officer responsible for implementing the AML/CFT/CPF framework and for liaison with FIU-IND and other competent authorities. The Principal Officer shall have sufficient authority, access to information and resources to perform the role effectively.

4.4 Compliance / Operations / Front Office

- Collect and verify KYC information and supporting documents.
- Follow customer acceptance and escalation procedures.
- Identify unusual activity and promptly escalate alerts to the Principal Officer/Compliance.
- Do not disclose STR-related information to clients or unauthorised persons.

4.5 Internal Audit / Independent Testing

Internal Audit or an independent competent function shall periodically test the design and operating effectiveness of AML/CFT/CPF controls, including KYC, risk classification, transaction monitoring, alerts, STR processes, sanctions screening, record retention and staff training.

5. Enterprise-Wide ML/TF/PF Risk Assessment

The Company shall conduct and document an enterprise-wide risk assessment appropriate to its size, business model, products, client base, geographies, delivery channels and transaction profile. The assessment shall identify, assess and mitigate money-laundering, terrorist-financing and proliferation-financing risks and shall be reviewed at least annually and when material changes occur.

Risk factors may include customer type, geography, occupation/business, source of funds/wealth, ownership/control structure, products and services, transaction volume/value, delivery channels, use of intermediaries, non-face-to-face relationships, PEP status, sanctions exposure and adverse information.

6. Customer Acceptance Policy

- No account shall be opened in an anonymous, fictitious or benami name.
- The Company shall not establish or continue a relationship where required CDD cannot be completed or where the identity of the client/beneficial owner cannot be satisfactorily established.
- High-risk relationships shall require enhanced due diligence and appropriate senior-management approval.
- The Company may decline, restrict or terminate a relationship where legal, regulatory, AML/CFT/CPF or reputational risks cannot be adequately mitigated.
- The Company shall apply additional controls where the client, beneficial owner, authorised person or relevant connected party presents sanctions, PEP, adverse-media or other elevated risk.

7. Customer Due Diligence (CDD) and KYC

The Company shall conduct CDD at onboarding and at appropriate intervals thereafter, and whenever there is a material change or trigger requiring re-verification. CDD shall include identification and verification of the client using reliable and independent sources, understanding the purpose and intended nature of the relationship, determining whether the client acts for another person, identifying and verifying beneficial ownership/control where applicable, and obtaining information necessary for risk assessment.

CDD shall be aligned with applicable SEBI KYC requirements, including KYC records and registration requirements applicable through KYC Registration Agencies and CKYCRR, as relevant.

Typical KYC information may include PAN, proof of identity/address, constitution documents, bank details, occupation/business profile, tax residency information, beneficial ownership/control details, authorised signatory

information and other documents required by law or the Company's risk assessment.

8. Beneficial Ownership

For legal persons and arrangements, the Company shall identify and take reasonable measures to verify the natural person(s) who ultimately own or control the client, in accordance with applicable PML Rules and regulatory requirements. Ownership/control structures shall be documented, including intermediate entities where relevant.

Where beneficial ownership cannot be satisfactorily established, the relationship shall be escalated to Compliance/Principal Officer and shall not proceed or continue unless the risk is appropriately resolved and permitted by applicable law.

9. Risk Classification

Clients shall be classified as Low, Medium or High risk, or under any more granular risk methodology adopted by the Company. Risk classification shall be based on documented factors and shall not be determined solely by a single factor.

Indicative higher-risk factors include PEP exposure, complex or opaque ownership, high-risk jurisdictions, adverse regulatory/criminal information, unusual source of funds/wealth, non-face-to-face risk, unexplained high-value activity, unusual third-party funding, sanctions concerns and patterns inconsistent with the stated profile.

Risk classification shall be reviewed periodically and whenever a material trigger occurs. High-risk clients shall be subject to enhanced due diligence and more frequent review.

10. Enhanced Due Diligence (EDD)

- Obtain additional identification, ownership/control and business information.
- Establish and, where appropriate, corroborate source of funds and source of wealth.
- Obtain senior management approval before establishing or continuing a high-risk relationship where required.
- Increase frequency and depth of transaction monitoring and KYC refresh.
- Conduct enhanced adverse-media and sanctions/PEP screening as appropriate.
- Document the rationale for accepting, continuing, restricting or terminating the relationship.

11. Politically Exposed Persons (PEPs)

The Company shall identify PEPs and relevant family members/close associates as required under applicable law and shall apply enhanced measures, including senior management approval, reasonable measures to establish source of wealth/source of funds and enhanced ongoing monitoring, as applicable.

12. Sanctions, Terrorist Financing and Proliferation Financing

The Company shall maintain screening and escalation controls appropriate to its business to identify persons and entities subject to applicable Indian and other legally binding sanctions/proscription requirements. Potential matches shall be investigated promptly. The Company shall take action required by law, including freezing/restriction/reporting where mandated, and shall maintain an auditable record of the review.

13. Transaction Monitoring

The Company shall maintain risk-based systems and procedures for monitoring transactions and client activity. Monitoring may include automated or manual review of trading, funds movements, securities transfers, pay-in/pay-out activity, third-party activity, account changes and other relevant events.

Examples of red flags include: activity inconsistent with the client profile; rapid movement of funds or securities without an apparent legitimate purpose; repeated transactions just below reporting/monitoring thresholds; unusual third-party payments; frequent changes in bank accounts; unexplained cross-border activity; complex or circular transactions; sudden large turnover; transactions with no apparent economic rationale; or attempts to avoid CDD or provide requested information.

14. Suspicious Transaction Identification and Investigation

A transaction may be suspicious regardless of its value and whether it is completed or attempted. Staff shall escalate unusual activity promptly. The Principal Officer/Compliance shall assess the available information, obtain supporting records, document the rationale and determine whether an STR or other report is required.

The Company shall not delay reporting merely because a transaction is incomplete or because the client provides an explanation, where the overall circumstances continue to indicate suspicion.

15. Reporting to FIU-IND

- Prescribed reports shall be furnished to FIU-IND in the required manner and within applicable statutory timelines.
- Suspicious Transaction Reports shall be furnished promptly and not later than seven working days after the Principal Officer is satisfied that the transaction is suspicious, in accordance with applicable requirements.
- Monthly reports for prescribed transaction categories shall be filed by the 15th day of the succeeding month, where applicable.
- The Company shall also comply with applicable reporting requirements for other prescribed transaction categories and thresholds.
- The Company shall retain evidence of report preparation, review, approval and submission.

16. No Tipping-Off

No director, employee, authorised person or other representative shall disclose to a client or any unauthorised person that an STR has been filed, is being considered, or that information relating to a suspected transaction has been furnished to FIU-IND, except where disclosure is expressly permitted by law.

17. Record Keeping and Retention

The Company shall maintain transaction records and CDD/KYC records in accordance with the PMLA, PML Rules, SEBI requirements and other applicable record-retention requirements. Records shall be sufficient to reconstruct individual transactions and to respond promptly to lawful requests from SEBI, FIU-IND, enforcement agencies, exchanges, depositories or other competent authorities.

Records shall be protected against unauthorised alteration, destruction or access and shall remain readily retrievable for the applicable retention period.

18. Confidentiality and Data Security

- AML/KYC and investigation records shall be accessible only to authorised personnel.
- Electronic records shall be protected using appropriate access controls, authentication, backups and audit trails.
- Physical records shall be stored securely with controlled access.
- Information shall be disclosed to regulators/law-enforcement authorities only through authorised channels and as legally required.

19. Correspondent / Intermediary / Third-Party Risk

Where the Company uses authorised persons, intermediaries, vendors or other third parties in processes relevant to AML/CFT/CPF, the Company shall conduct appropriate due diligence, define responsibilities contractually, monitor performance and ensure that ultimate regulatory responsibility is not improperly delegated.

20. Employee Screening and Training

Employees and relevant personnel shall receive AML/CFT/CPF training appropriate to their roles. Training shall cover customer identification, red flags, escalation, sanctions/PEP screening, transaction monitoring, record keeping, confidentiality and tipping-off. Training completion shall be documented. Appropriate employee screening shall be undertaken consistent with law and the Company’s HR controls.

21. Internal Controls, Testing and Audit

The Company shall maintain documented AML/CFT/CPF procedures, escalation matrices, maker-checker controls where appropriate, exception reports and management information. Independent testing shall assess whether controls operate effectively and whether identified deficiencies are remediated within defined timelines.

22. Whistleblowing and Escalation

Employees may report suspected AML/CFT/CPF breaches or control weaknesses through the Company's compliance/whistleblower channels. Retaliation against a person who raises a concern in good faith is prohibited, subject to applicable law and the Company's policies.

23. Business Exit / Account Closure

Where a relationship is closed for AML/CFT/CPF reasons, the Company shall follow applicable legal and regulatory requirements, preserve records, manage outstanding obligations and avoid tipping-off. Where required, the matter shall be escalated to the Principal Officer for consideration of regulatory reporting.

24. Red-Flag Indicators – Illustrative List

- Client refuses or repeatedly delays KYC/beneficial-owner information.
- Identity documents or ownership information appear inconsistent or unverifiable.
- Trading activity is materially inconsistent with the stated occupation, financial profile or investment objective.
- Large or frequent transactions without an apparent legitimate economic purpose.
- Frequent third-party deposits/payments or unexplained changes in bank accounts.
- Rapid in-and-out movement of funds or securities with limited investment rationale.
- Use of multiple accounts or entities that appear linked without a clear purpose.
- Unusual cross-border activity, high-risk jurisdiction exposure or sanctions concerns.
- Repeated attempts to structure transactions to avoid scrutiny or reporting.
- Unusual activity immediately after onboarding, KYC update, bank-account change or dormant-account reactivation.
- Attempts to induce employees to bypass KYC, transaction controls or approval procedures.

Approval Signatures

Designated Director: RAMESH PARDIWALA_____Date: 01-04-2025

Principal Officer:RAHUL PARDIWALA _____Date: 01-04-2025

For Pardiwala Securities Pvt Ltd