PARDIWALA SECURITIES PVT LTD

FRAUD PREVENTION & DETECTION POLICY

1. Purpose

This Policy establishes the framework adopted by **Pardiwala Sec Pvt Ltd** for prevention, detection, escalation, investigation and reporting of fraud and market abuse.

The Policy is intended to protect clients, investors, the Company and the integrity of the securities market by establishing appropriate surveillance systems, internal controls, employee obligations, escalation mechanisms and a whistle-blower framework.

2. Regulatory Framework

The Policy is framed with reference to applicable provisions of the SEBI Act, 1992, Securities Contracts (Regulation) Act, 1956, SEBI (Stock Brokers) Regulations, 2024 and amendments, SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003, applicable exchange/clearing corporation rules and circulars, and other applicable laws and regulatory directions.

SEBI Circular No. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/96 dated 4 July 2024 requires stock brokers to establish an institutional mechanism for prevention and detection of fraud or market abuse, including surveillance and internal controls, obligations of the broker and employees, escalation/reporting mechanisms and a whistle-blower policy.

3. Scope

This Policy applies to the Company, its directors/partners/proprietor, key managerial personnel, compliance and risk functions, dealers, employees, authorised persons, consultants/outsourced personnel where relevant, and activities undertaken on behalf of or through the Stock Broker.

It covers client onboarding and account activity, orders and trades, proprietary trading where applicable, employee trading, market-facing communications, handling of client funds/securities, technology and access controls, and interactions with exchanges, clearing corporations, depositories, regulators and other intermediaries.

4. Definitions

Fraud: Fraud shall have the meaning assigned under applicable securities laws, including the SEBI PFUTP Regulations, as amended from time to time.

Market Abuse: Includes manipulative, fraudulent or unfair trading practices, including activity involving mule accounts, as applicable under the Broker Regulations.

Red Flag: An unusual, suspicious or inconsistent activity that may indicate fraud, market abuse, unauthorised activity, misuse of systems or other regulatory concern.

Whistle-blower: Any person who, in good faith, reports a suspected violation, fraud, market abuse or other misconduct under this Policy.

5. Policy Principles

Zero tolerance for fraud, market manipulation, unauthorised trading and deliberate misuse of client or Company assets.

Risk-based surveillance and controls proportionate to the Company's business, client base, products and risk profile.

Prompt escalation of material or suspicious matters to the designated authority and, where required, to exchanges, SEBI or other competent authorities.

Protection of confidentiality and prohibition of retaliation against persons making bona fide reports.

Maintenance of adequate records and audit trails to support monitoring, investigation and regulatory reporting.

6. Governance & Responsibilities

Board / Governing Body: Approves the Policy, oversees the effectiveness of the institutional mechanism and receives material fraud/market-abuse reports.

Compliance Officer: Oversees regulatory compliance, coordinates escalation/reporting, maintains appropriate records and independently raises material non-compliance.

Risk / Surveillance Function: Conducts monitoring, reviews alerts, identifies patterns and escalates exceptions.

Operations & Technology: Maintains maker-checker controls, access controls, system logs, reconciliation and data integrity.

Employees & Dealers: Follow controls, avoid conflicts and unauthorised activity, preserve confidentiality and promptly report concerns.

Authorised Persons / Business Associates: Comply with applicable requirements and cooperate with surveillance and investigation.

7. Surveillance & Internal Controls

The Company is maintain systems and controls reasonably designed to detect, prevent and report potential fraud or market abuse by clients, employees, authorised persons or other relevant persons.

Monitoring may include, as appropriate: unusual order/trade patterns; wash/circular or self trades; spoofing/layering; pump-and-dump indicators; price/volume anomalies; front-running indicators; suspected insider trading indicators; unauthorised trading; excessive order modifications/cancellations; unusual use of dormant/inactive accounts; mule-account indicators; rapid fund/securities movements; third-party payment concerns; and activity inconsistent with the client's profile.

Controls shall include appropriate segregation of duties, maker-checker approvals, privileged-access management, user authentication, system and dealer logs, reconciliation of funds/securities, exception reporting, periodic access reviews and business continuity arrangements.

8. Client & Account-Level Controls

The Company isl conduct applicable KYC, client due diligence and risk assessment in accordance with law and applicable regulatory requirements.

Accounts and transactions may be subject to enhanced review where there are unusual patterns, inconsistent financial profiles, suspicious fund flows, multiple related accounts, frequent changes in contact/bank details, third-party payment concerns or other risk indicators.

Where permitted and required, transactions or access may be restricted, escalated or subjected to enhanced due diligence pending review.

9. Employee & Dealer Obligations

Employees and dealers shall not engage in front-running, insider trading, market manipulation, unauthorised trading, misuse of confidential information, preferential treatment, mis-selling or any activity that may compromise market integrity.

Employees shall comply with the Company's code of conduct and personal trading requirements, disclose conflicts of interest, protect confidential information and cooperate with surveillance and investigations.

Any employee who becomes aware of suspected fraud or market abuse must promptly report it through the designated internal channel.

10. Red Flags & Alert Handling

Alerts shall be risk-ranked and reviewed within a reasonable timeframe based on severity. Higher-risk alerts shall be escalated immediately or as required by internal procedures.

Review may include client profile, historical trading, order/trade data, related accounts, device/IP information where lawfully available, fund/security movement, employee involvement, communications and other relevant records.

Alerts shall be closed only after documented review and rationale. Where concerns remain, the matter shall be escalated for investigation and regulatory reporting as applicable.

11. Escalation & Reporting

Material or credible instances of suspected fraud or market abuse shall be escalated to the Compliance Officer / designated senior authority without undue delay.

The Company shall make reports, disclosures or notifications to SEBI, stock exchanges, clearing corporations, depositories, law-enforcement agencies or other competent authorities where required under applicable law or regulatory directions.

Regulatory reporting shall be accurate, complete, timely and supported by relevant records.

12. Investigation

Investigations shall be conducted objectively and confidentially. The Company may review orders, trades, logs, communications, account records, approvals, access records and other relevant evidence, subject to applicable law.

Persons involved may be asked to provide explanations or records. Investigations shall preserve evidence and maintain an appropriate audit trail.

Where warranted, remedial or disciplinary action may be taken in accordance with applicable law, employment/contractual terms and Company procedures.

13. Whistle-Blower Policy

The Company isl provide a channel through which employees, clients, authorised persons and other stakeholders may report suspected fraud, market abuse, misconduct or control failures in good faith.

Reporting channel: [dedicated email / postal address / telephone].

Reports may be made confidentially, subject to legal requirements. Anonymous reports may be accepted where permitted by the Company's procedures.

Retaliation, victimisation or adverse action against a person making a bona fide report is prohibited. Deliberately false or malicious complaints may be subject to appropriate action.

14. Confidentiality & Data Protection

Information relating to alerts, investigations, whistle-blower reports and regulatory matters shall be restricted to personnel with a legitimate need to know.

Records and personal information shall be handled in accordance with applicable privacy, data-protection, securities-market and record-retention requirements.

15. Record Retention

The Company shall maintain records relating to surveillance, alerts, investigations, decisions, escalations, reports and supporting evidence for the period prescribed under applicable laws, regulations, exchange requirements and the Company's record-retention policy.

16. Training & Awareness

Relevant employees shall receive periodic training on fraud risks, market abuse, red flags, surveillance escalation, conflicts of interest, whistle-blower protections, information security and regulatory obligations.

Training completion and supporting records shall be maintained.

17. Periodic Review & Testing

The Policy and associated controls shall be reviewed at least annually and earlier where there is a material regulatory, business, technology or risk change.

Surveillance rules, access controls and key fraud-prevention controls shall be periodically tested. Deficiencies shall be documented, assigned to responsible persons and tracked to closure.

18. Non-Compliance

Failure to comply with this Policy may result in disciplinary action, suspension/restriction of access or business activity, termination of employment/association, regulatory reporting and/or other action as permitted by law.

19. Contact for Reporting

Fraud / Market Abuse Reporting: RAHUL PARDIWALA / COMPLAINCE OFFICER
Email: rahul@rkpspl.com
Telephone: 022 22651196
Postal Address: **R**egistered/corporate office address

Clients should use the Company's official grievance mechanism for investor complaints. Regulatory grievance mechanisms, including SEBI's SCORES platform, may be used where applicable after following the prescribed process.

****