Surveillance Policy

Entity Name	Manog Securities Pvt Ltd
SEBI Registration No.	INZ000278434
Compliance Officer	Pawan Pratap Singh
Date of Adoption	28-JAN-2026

1. Scope

Manog Securities Pvt Ltd frames this Surveillance Policy in compliance with Exchange and SEBI rules, to monitor trading activity — both client-facing and proprietary — and detect manipulative, abusive, or suspicious patterns.

2. Exchange-Provided Transactional Alerts

The Compliance Officer shall download and review the following alerts daily from the Exchange system:

Sr.	Alert Type	Segment	Applies To
1	Significant increase in activity	All Segments	Client + Proprietary
2	Sudden activity in dormant account	All Segments	Client
3	Clients / Group dealing in common scrips	Equity / Derivatives	Client
4	Concentration in illiquid scrips / contracts	Derivatives / Commodity	Client + Proprietary
5	Trading at minimum lot size	Derivatives / Commodity	Client + Proprietary
6	Concentrated position in a scrip	All Segments	Client + Proprietary
7	Circular Trading	All Segments	Client + Proprietary
8	Pump and Dump	Equity / Derivatives	Client + Proprietary
9	Wash Sales	All Segments	Client + Proprietary
10	Reversal of Trades	All Segments	Client + Proprietary
11	Front Running	All Segments	Client + Proprietary
12	Concentrated Open Interest / High Turnover	Derivatives / Commodity	Client + Proprietary

Registered Office : C-3/3089, Vasant Kunj, New Delhi-110070
Ph. : +91-11-42860133, 41099295, 41676280, 41824213, 41016593
E-mail : manog@manogsecurities.com

13	Order Book Spoofing	All Segments	Client + Proprietary
14	High order-to-trade ratio (Algo)	All Segments — Algo	Client + Proprietary
15	Commodity delivery default / warehouse irregularity	Commodity	Client + Proprietary
16	Commodity price band breach	Commodity Derivatives	Client + Proprietary

3. Client Account Surveillance

3.1 KYC and UCC Maintenance

- KYC parameters updated annually — latest information uploaded to Exchange UCC database
- Groups / associations established amongst related client accounts: common email, mobile, address, UCC linkages — to identify multiple/common accounts

3.2 Alert Analysis Procedure

- Record alert in Surveillance Register: date, type, client code(s), scrip/contract
- Seek explanation from identified client(s) for entering into such transactions
- Seek bank statements and demat statements for at least 15 days from transaction date — verify settlement funds belong to the client
- Review: alert type, client financial profile, past trading pattern, bank/demat details, connected UCCs, public information
- Record written observations for all identified transactions
- Report adverse findings to Exchange within **45 days** of alert generation
- If suspicious/manipulative activity confirmed: file STR with FIU-IND via FINnet 2.0 within **7 days** of conclusion

4. Proprietary Trading Surveillance

- Daily order-to-trade ratio across all segments — flag if unusually high (spoofing indicator)
- Intra-day pattern of orders placed and cancelled in rapid succession — screen for layering
- Own position concentration relative to Exchange-wide open interest — ensure position limits not breached
- Dealer-level anomaly: override of pre-trade controls, unusual end-of-day position changes
- Any proprietary order pattern mirroring a pending client order — reviewed for

front-running risk

5. Algorithmic / API Trading Surveillance

Algo / API Trading: **Not Applicable**

If Applicable:

- Daily review of algo order-to-trade ratios vs. Exchange-prescribed thresholds
- Kill-switch test: [frequency, e.g., Monthly] — document results
- Monitor for dysfunctional algo: loop execution, runaway orders, erroneous price breaches
- Black-box algo provider must hold valid SEBI Research Analyst registration — verify annually

6. Employee Communication Monitoring — Para 85

- No employee or AP shall circulate unverified market-sensitive information through any channel — **email, WhatsApp, Telegram, social media, chat forums, or messaging apps**
- Market-related communication to clients from verified, publicly available sources only
- Annual training on this prohibition — minimum **1 hour**. Attendance mandatory. Records maintained for 5 years

7. Alert Disposal and Governance

Activity	Timeline	Responsible
Download Exchange alerts	Daily — before start of trading session	Compliance Officer
Dispose of / close each alert	Within 30 days (document delay reasons)	Compliance Officer
Critical alerts internal escalation	Within 24-48 hours	Compliance Officer → Partners
Report adverse findings to Exchange	Within 45 days of alert generation	Compliance Officer

File STR (if suspicious activity confirmed)	Within 7 days of conclusion	Principal Officer via FINnet 2.0
Quarterly MIS to Board / Partners	Within 15 days of quarter end	Compliance Officer
Internal Audit review of Surveillance	Each half-year	Internal Auditor

8. Surveillance Register — Mandatory Fields

Field	Description
Alert Date	Date the alert was downloaded from Exchange
Alert Type	Type as per Exchange classification
Client Code(s) / Account	UCC(s) or own account involved
Scrip / Contract	Security / commodity / contract to which alert relates
Analysis Summary	Documents obtained, client explanation, findings
Observation	Adverse / No Adverse Finding
Action Taken	Closed / Reported to Exchange / STR Filed / Escalated
Date of Disposal	Date alert was fully closed or reported
Delay Reason (if beyond 30 days)	Documented reason for delay

9. Quarterly MIS to Board / Partners

Placed before Partners / Board within 15 days of each quarter end. Must include:

- Alerts downloaded by type and segment
- Alerts disposed with no adverse finding
- Alerts reported to Exchange — with outcome
- STRs filed (if any — without confidential details)
- Alerts pending with reasons and expected disposal date
- Front-running / proprietary conflicts identified and resolved
- Employee communication violations and actions taken

- Algo kill-switch test results (if applicable)

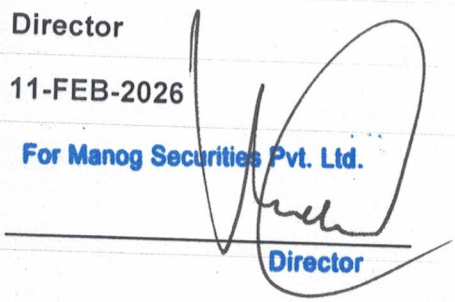
10. Internal Audit Scope

- Completeness of Exchange alert downloads — verify against Exchange-generated alert summary
- Quality of alert disposals — sample review for adequacy of analysis
- Timeliness — flag disposals beyond 30 days without documented reason
- Adverse findings reported within 45 days — verify timeliness
- STRs — verify 7-day compliance
- Employee communication monitoring — training records and disciplinary actions
- Algo surveillance — OTR logs and kill-switch test records (if applicable)
- Proprietary vs. client order conflict checks — no front-running pattern

Policy Review

Last Reviewed	**11-FEB-2026**
Reviewed By	**Pawan Pratap Singh (Compliance Officer)**
Approved By	**Director**

For and on behalf of: Manog Securities Pvt Ltd

Authorised Signatory	**Mr. Vivek Gupta**
Designation	**Director**
Date	**11-FEB-2026**
Signature	**For Manog Securities Pvt. Ltd.**  **Director**