

SURVEILLANCE POLICY

1. Regulatory Framework & Objective

This policy is established to detect and prevent market abuse, insider trading, and fraudulent activities. It complies with:

- SEBI Circular on Institutional Mechanisms for Prevention and Detection of Fraud or Market Abuse.
- NSE Master Circulars on Surveillance & Investigation Protocols.

As mandated by the NSE, this policy must be reviewed at least annually and formally approved by the broker's **Board of Directors / Apex Body**.

2. Dual-Source Alert Mechanism

The Surveillance Desk tracks market activities through two distinct transaction streams:

2.1 Exchange-Downloaded Alerts

The firm processes transaction alerts provided directly by the NSE through the electronic member portals. These templates focus on:

- **Concentration Alerts:** A single client or connected group executing an unusually high percentage of market volume in a specific scrip.
- **Day Trading In Illiquid Scripts:** Abnormal price-to-volume spikes driven by a single retail account.
- **Sudden Active Trading:** High-volume buy/sell execution originating from long-dormant Unique Client Codes (UCC).

2.2 Broker Internal Surveillance Generation

Independent of exchange portals, the internal risk management software must generate independent daily triggers. The core internal themes are:

[Internal Transactional Scans] —> [Flagged Multi-UCC Data] —> [Due Diligence Check] —> [MSD/FIU Reporting]

- **Circular / Synchronized Trading:** Reversing matching order executions between identical counter-parties within a narrow time window.
- **Pump-and-Dump Flags:** Clients driving high purchase volumes in penny stocks (Z-Group / ASM / GSM) followed by sudden delivery liquidations.

- **Cross-Logins (Single IP/Location Mapping):** Multi-UCC accounts placing trades simultaneously from a single external IP address or physical location.
-

3. Step-by-Step Due Diligence & Disposal Process

When an internal or exchange alert triggers, the surveillance team executes a strict, documented workflow:

Step 1: Preliminary Data Collation (Within T+2 Days)

The analyst reviews the client's UCC master profile, historical trading records, past alert history, and physical geolocation logs.

Step 2: Financial Consistency Review

The team evaluates if the trade volume matches the client's declared net worth or income slips submitted during onboarding.

Step 3: Formal Client Clarification Request

If an anomaly is detected, an electronic request is sent to the client's registered email address. The client must submit a valid commercial explanation and supporting bank/demat statements within **3 working days**.

Step 4: Final Closure Decisions

- **Disposed Alerts:** If the trading behavior is backed by valid economic rationale, the alert is closed. The detailed analysis and reasons are recorded in the internal system logs.
 - **Escalated Alerts:** If the client provides false or evasive details, the case moves to the **Principal Officer**.
-

4. Mandatory Regulatory Reporting Timelines

In line with NSE surveillance dashboard specifications, reporting follows strict timelines:

Reporting Portal / Target	Mandated Reporting Frequency	Action Taken Criteria
NSE Member Surveillance Dashboard (MSD)	Quarterly Submission (Within 15 days of quarter end)	Upload details of internally generated alerts and their disposal justifications.

FIU-IND FINNET Portal	Within 7 Working Days of confirmation	File a formal Suspicious Transaction Report (STR) for verified fraudulent/laundered transactions.
------------------------------	--	---

5. Data Sovereignty & Audit Mandates

- **No Tipping Off:** Employees must ensure that clients are never notified or "tipped off" that their accounts are under active surveillance audit or being processed for an STR filing.
- **The 8-Year Record Archival:** All documentation, client emails, system alert records, analysis notes, and disposal logs must be stored in an unalterable digital archive for a minimum of **8 years**.
- **System Audit:** The surveillance application architecture, logic matrices, and compliance tracking workflows are reviewed annually by an independent system auditor or specialized Chartered Accountant.

