

Surveillance Policy

1. Introduction

Unique Stockbro Private Limited (hereinafter referred to as the "Company") has formulated this Surveillance Policy (hereinafter referred to as the "Policy") in accordance with the directives and circulars issued by regulatory authorities including Central Depository Services (India) Limited (CDSL), National Stock Exchange of India Limited (NSE), and BSE Limited (BSE).

Recently Central Depository Services India Limited (for the sake of brevity hereinafter referred to as "**CDSL**"), National Stock Exchange of India Limited (for the sake of brevity hereinafter referred to as "**NSE**") and BSE Limited (for the sake of brevity hereinafter referred to as "**BSE**") issued circulars directing intermediaries to put in place a surveillance framework due to which need has arisen to modify/ revise existing Surveillance Policy. Hence this policy is framed division wise in order to incorporate requirements of each division.

2. SURVEILLANCE FRAMEWORK – DEPOSITORY PARTICIPANT (DP) DIVISION

2.1. Regulatory Basis

Pursuant to CDSL Communiqué No. CDSL/OPS/DP/SYSTM/2021/309 dated July 15, 2021, all depository participants are mandated to implement an effective surveillance mechanism to monitor client behavior and report anomalies.

2.2. Key Surveillance Obligations

- Generation of surveillance alerts as detailed in Section 2.4
- Timely disposal of all alerts within 30 calendar days of their generation
- Documentation of reasons for any delay in alert disposition
- Escalation and reporting of abnormal/ suspicious activities to CDSL or other relevant authorities
- Maintenance of comprehensive records for the statutory period prescribed under applicable laws including PMLA

2.3. Client due diligence

DP Division shall perform ongoing due diligence of clients, including:

- Periodic updating of Know Your Client (KYC) details in accordance with SEBI guidelines
- Verification of income, net worth, and other demographic and financial details
- Continuous review of client activity to assess risk and detect anomalies
- In addition to the transactional alerts downloaded from the Exchanges, DP Division shall also generate appropriate surveillance alerts under the following circumstances/ themes to effectively monitor client activities at their end, in accordance with the Surveillance Policy. Such alerts may also be generated if any suspicious, unusual, or non-routine trading activity is observed that deviates from normal or expected client behavior/ profile.

2.4. List of Surveillance Alerts

Sr. No.	Consolidated Surveillance Themes / Alerts
A.	Client On-boarding & KYC-Related Alerts
	Multiple Demat Accounts with Same Demographics: Accounts opened with common mobile number, email ID, bank account number, or address, considering existing accounts with the DP
	Bounced Communication: Alerts where emails or letters sent to clients on their registered correspondence details are returned / bounced
	Frequent Changes in Account Details: Multiple changes in address, email ID, mobile number, authorized signatory, or POA holder in a short period
	Abnormal Activity in New Accounts: Newly opened accounts showing a burst of activity followed by zero holdings or dormancy
	Short-Lived Accounts: Accounts opened and closed within a short duration
B.	Off-Market, Demat & Pledge-Related Alert
	Frequent Off-Market Transfers: A high number of off-market transactions by a client in a defined timeframe
	Disproportionate Off-Market Transfers: Off-market transactions not aligned with the declared income or net worth of the client
	Disproportionate Pledge Transactions: Pledge activity not commensurate with

	client's financial profile
	High-Value Transfers After Modification: Large off-market transactions occurring immediately after updates to client details
	Inconsistent Off-Market Transfer Reasons: Reason codes like gifts or donations to unrelated parties or frequent off-market sales inconsistent with client profile
	High Volume / Value Dematerialization: Unusually large or frequent demat transactions
	Transactions in Dormant Accounts: Activity in accounts classified as dormant
	Unusual High Credit: High value or volume credits, gifts, or donations not aligned with client profile
	Unusual High Debit: High value or volume debits, gifts, or donations sent out, possibly suspicious
	GSM / ASM Scrip Transfers: High volume / value off-market transactions in securities listed under GSM or ASM watch lists by exchanges
	Significant Holdings in Listed Scrips: Clients holding disproportionately high stakes in listed companies
C.	Market behaviour & Trading Pattern Alerts
	Client/ group of clients, as identified by the trading member, accounting for a significant percentage of the total trading activity in a scrip / contract as compared to the market
	Client/ group of clients with new account(s) or clients dealing after a significant time gap, as identified by the trading member, accounting for significant value / percentage of total trading activity in a scrip / contract as compared to the market
	Client/ group of clients dealing frequently in small quantities/minimum market lot in a scrip/ contract.
	Disproportionate trading activity vs reported income / Net worth.
	Client/ group of clients having any possible direct or indirect connection with the said listed company, undertaking suspicious trading activity prior to the dissemination of the price-sensitive announcement
	Client/ group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list'.
	Consistency in profit / loss at client / group of clients' levels, rationale for such trading activities
	Significant trading activity in scrips by client who has pledged the shares of same scrip.
	Monitoring whether orders placed by respective clients or authorized representatives
	Monitoring client's address vis-à-vis dealing office address

	Trading activities of accounts of relatives to identify synchronized / coordinated trading
D.	Internet based Trading Surveillance
	Surveillance/ monitoring of IP or MAC addresses of clients
	Identification of multiple client codes trading from the same location
E.	Exchange driver Alerts & Threshold Review
	The Trading Members are also required to review and take the necessary action on the transactional alerts provided by the Exchanges
	Alerts as specified above to be monitored by the Trading Member on a monthly/daily basis.
	The Trading Member shall review and recalibrate, wherever required, the threshold set at least once in a year to ensure adequacy of the same.

2.5. Alerts generation and Reporting

- Alerts must be analyzed in the light of documentary evidence (demat statements, financials, etc.)
- Alerts must be reviewed based on facts, antecedents, and verification of relevant documents. The DP Division shall exercise its independent judgment and take appropriate action to detect any abnormal or suspicious transactions.
- Electronic registers must be maintained, recording all alerts, analysis, and outcomes
- All alerts from CDSL must be responded to with final status (Verified & Closed/ Verified & Reported) within 30 days
- Alerts with adverse observations generated internally must be reported to CDSL, within 7 days.

2.6. Obligations of the Compliance Officer

- The surveillance activities carried out by the DP Division shall be under the overall supervision and control of the Compliance Officer. The Compliance Officer shall ensure that all surveillance mechanisms are implemented in accordance with the Surveillance Policy and regulatory requirements.
- The Compliance Officer shall be responsible for overseeing the identification,

- escalation, and resolution of alerts generated through both Depository generated and/ or internally generated. Compliance Officer must ensure that adequate records are maintained and that appropriate actions are taken in a timely manner.
- A detailed Quarterly Management Information System (MIS) report shall be prepared and submitted to the Designated Director. The MIS shall contain:
 - Quarterly details of the Surveillance Alerts
 - a. Alerts under the process at the beginning of the quarter
 - b. Alerts generated during the quarter;
 - c. Alerts processed and acted upon during the quarter;
 - d. Alerts referred to the Exchange;
 - e. Alerts pending at the end of the quarter, along with justifications for the pendency and an action plan for their closure.
 - In addition, the Compliance Officer shall ensure that any exceptions, anomalies, or deviations observed during the processing or disposal of alerts are brought to the attention of the Designated Director as part of the MIS report or through a separate communication, as deemed appropriate.
 - A quarterly MIS shall be put up to the Designated Directors on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with reasons for pendency and action plan for closure. Also, the Designated Director shall be apprised of any exception noticed during the disposition of alerts.

2.7. Obligations of Designated Director

- The Designated Director shall bear overall responsibility for the effective implementation and oversight of the surveillance framework
- They shall ensure that adequate resources, systems, and controls are in place to monitor and detect abnormal or suspicious trading activities.
- The Designated Director shall periodically review the MIS reports submitted by the Compliance Officer, evaluate the action taken on alerts, and provide necessary guidance or directives for strengthening the surveillance process where required.

- It shall be the duty of the Designated Director to ensure that surveillance-related responsibilities are discharged in line with the applicable laws, rules, and regulatory expectations.

2.8. Obligations of Internal Auditor / Concurrent Auditor

- The Internal Auditor of the trading member shall be responsible for conducting an independent review of the Surveillance Policy, including its adequacy, implementation, and operational effectiveness.
- As part of the audit, the Internal Auditor shall verify whether the surveillance alerts—both from Depository and those generated internally—are being properly reviewed, investigated, and acted upon as per defined procedures.
- The auditor shall assess:
 - a. The timeliness and appropriateness of responses to surveillance alerts;
 - b. The documentation and escalation process;
 - c. The adequacy of records maintained;
 - d. The overall compliance with internal policies and external regulatory norms.
- All observations, findings, and recommendations related to the surveillance framework shall be duly documented in the Internal Audit Report, which shall be submitted to the management and Designated Director for review and corrective action, if necessary.

2.9. Obligation of Quarterly reporting of status of the alerts generated by DP Division:

A tabular format capturing lifecycle of alerts shall be submitted, including:

- Pending alerts at start of quarter
- New alerts during quarter
- Alerts verified and closed
- Alerts reported to depository
- Pending alerts (age-wise classification: <1 month, 1–2 months, etc.)

- Summary of significant surveillance actions taken
- A NIL report shall be submitted if no actionable items arise in a given quarter
- DP division is also required to provide duly approved status of the alerts on a quarterly basis, in the following format to CDSL within 15 days from end of the quarter

Format of Status of Alerts generated by the Depository:

Name of Alert	Alerts pending at the beginning of quarter (A)	Alerts generated during the quarter (B)	Total number of Alerts [(C) = (A)+(B)]	Number of Alerts Verified & closed during the quarter (D)	Number of Alerts reported to Exchanges / Depository (D1)	Alerts pending at the end of the quarter [(E) = (C)-(D)]	Ageing analysis of the alerts pending at the end of the Quarter [Segregation of E column]					Reasons for pendency
							< 1 months	1-2 months	2-3 months	3-6 months	> 6 months	

Details of any major surveillance action taken (other than alerts reported to Depository), if any, during the quarter:

Sr. No.	Brief action taken during the quarter

3. SURVEILLANCE FRAMEWORK – BROKING DIVISION (NSE & BSE)

3.1. Regulatory Basis:

- NSE Circular NSE/INVG/65921 dated December 31, 2024 – “Guidelines on Strengthening Surveillance Framework of Trading Members”
- Surveillance & Investigation Consolidated Circular No. NSE/SURV/61818 dated April 30, 2024
- BSE Notice No. 20210701-30 dated July 1, 2021, and subsequent amendments

These circulars mandate Trading Members to maintain robust, proactive, and risk-based surveillance controls, including independent alert generation, time-bound review, documentation, escalation, and governance oversight.

3.2. Key Surveillance Obligations

Broking Division shall ensure:

- Time-bound closure of Exchange-downloaded alerts within 45 days, as mandated.
- Internal alerts generated by the Broking Division shall be reviewed, analysed, closed, or escalated within 90 days of generation.
- Documented rationale for delayed review/closure, if any.
- Identification of manipulative, suspicious, concentrated, unusual, or pattern-based trading activities.
- Maintenance of complete audit trail, including all evidences, rationale, communications, KYC reviews, and action taken.
- Periodic review and annual update of the Surveillance Policy to reflect new risks, regulatory changes, or business developments.
- Ensuring the availability of adequate resources and systems to effectively monitor all client activities.

3.3. Internally Generated Surveillance Alerts

In addition to Exchange-generated alerts, the Broking Division shall independently generate surveillance alerts under the below mandatory themes, expanded in accordance with the prescribed guidelines.

Alerts shall be generated wherever unusual, non-routine, inconsistent, or suspicious behaviour is observed vis-à-vis normal client profile or market conditions.

The themes applicable to Broking division are given hereunder:

Surveillance Themes/ Alerts to be generated:

Sr. No.	Consolidated Surveillance Themes / Alerts
A.	Client On-boarding & KYC-Related Alerts
	Multiple Demat Accounts with Same Demographics: Accounts opened with common mobile number, email ID, bank account number, or address, considering existing accounts with the DP
	Bounced Communication: Alerts where emails or letters sent to clients on their registered correspondence details are returned / bounced
	Frequent Changes in Account Details: Multiple changes in address, email ID, mobile number, authorized signatory, Income range/ financial information or POA holder in a short period
	Abnormal Activity in New Accounts: Newly opened accounts showing a burst of activity followed by zero holdings or dormancy
	Dormant clients becoming active with significant market contribution
	Short-Lived Accounts: Accounts opened and closed within a short duration
B.	Market behaviour & Trading Pattern Alerts
	Client/ group of clients, as identified by the trading member, accounting for a significant percentage of the total trading activity in a scrip/ contract as compared to the market
	Client/ group of clients with new account or clients dealing after a significant time gap, as identified by the trading member, accounting for significant value/ percentage of total trading activity in a scrip/ contract as compared to the market
	Client/ group of clients dealing frequently in small quantities/ minimum market lot in a scrip/ contract
	Disproportionate trading activity vs reported income/ Net worth
	Client(s) or group of clients having any possible direct or indirect connection with the said listed company, undertaking suspicious trading activity prior to the dissemination of the price-sensitive announcement
	Client/ group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list' or ASM & GSM/ Graded Surveillance scrips
	Consistency in profit / loss at client / group of clients' levels, rationale for such trading activities
	Cross-market pattern (Cash + Derivatives) where behaviour in one segment influences the other (New requirement)
	Significant trading activity in scrips by client who has pledged the shares of same scrip
	Pattern of pledging and immediate selling, potentially indicating funding-led trades
	Rapid build-up/ unwinding in F&O inconsistent with client profile

Sr. No.	Consolidated Surveillance Themes / Alerts
	Monitoring whether orders placed by respective clients or authorized representatives
	Orders placed by persons other than the client; mismatches between KYC address and dealing location/terminal/IP
	Trading Pattern Mismatch with Financial Profile: Disproportionate activity vs declared income / net worth
	Frequent or unusually large MTM gains/losses
	Structured daily profits with minimal risk
	Monitoring client's address vis-à-vis dealing office address
	Unusual Activity in IPO-Listed Scrips - Concentration and price-impacting trades in newly listed securities, especially early listing days
	Trading activities of accounts of relatives to identify synchronized / coordinated trading
C.	Internet based Trading Surveillance
	Surveillance / monitoring of IP/ MAC addresses of clients
	Identification of multiple client codes trading from the same location
D.	Exchange driver Alerts & Threshold Review
	The Trading Members are also required to review and take the necessary action on the transactional alerts provided by the Exchanges
	Alerts as specified above to be monitored by the Trading Member on a monthly/daily basis
	The Trading Member shall review and recalibrate, wherever required, the threshold set at least once in a year to ensure adequacy of the same
E.	Algo-Related Surveillance Events
	Unusual algo usage
	Frequent algo parameter changes
	Abnormal order-to-trade ratio
F.	Structured / Circular / Synchronized Activity
	Wash trades
	Reversal trades
	Self-trades
G.	Order Book Manipulation Alerts

Sr. No.	Consolidated Surveillance Themes / Alerts
	Spoofing
	Layering
	Frequent Placing and cancellation of large orders
	Placing orders away from LTP to influence price

The Broking Division shall analyse all such alerts based on facts, client profile, risk category, documents such as bank statements / demat statements, and apply professional judgment to determine necessary action.

3.4. Due Diligence

The following activities required to be carried out by the broking division for client due diligence:

- Conduct continuous, ongoing due diligence of all clients.
- Periodically update key KYC parameters as per SEBI KYC/KRA guidelines.
- Review income, financial capacity, trading patterns, and deviations from the client's profile.
- Establish groups/associations across clients based on addresses, patterns, mobile numbers, introducers, or other parameters.
- Apply enhanced due diligence for high-risk or unusual behaviour, including additional documentation wherever required.

3.5. Obligation of Broking division with respect to processing of alerts:

- Obtain trading rationale and supporting documents such as bank statements, demat statements, financials, etc.
- Record a detailed note of observations, analysis, and conclusion for each alert.
- Close or escalate all Exchange-generated alerts within 45 days, updating the Member Surveillance Dashboard.

- Review internally-generated alerts and report adverse observations to the Exchange within 90 days.
- Maintain proper audit trail, including screenshots, documents, emails/SMS/telephone logs, and rationale for decision.

3.6. Obligations of Compliance officer

- Exercise overall supervision and ensure full implementation of the Surveillance Policy.
- Oversee timely evaluation, closure, and escalation of alerts.
- Ensure proper documentation, evidence collection, and updating of the Member Surveillance Dashboard.
- Ensure compliance with SEBI and Exchange requirements at all times.
- Prepare a detailed **Quarterly MIS** for the Designated Director, containing:
 - a. The number of surveillance alerts pending at the beginning of the quarter;
 - b. Alerts generated during the quarter;
 - c. Alerts processed and acted upon during the quarter;
 - d. Alerts referred to the Exchange;
 - e. Alerts pending at the end of the quarter, along with justifications for the pendency and an action plan for their closure.
- In addition, the Compliance Officer shall ensure that any exceptions, anomalies, or deviations observed during the processing or disposal of alerts are brought to the attention of the Designated Director as part of the MIS report or through a separate communication, as deemed appropriate.
- A quarterly MIS shall be put up to the Designated Directors on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with reasons for pendency and action plan for closure. Also, the Designated Director shall be apprised of any exception noticed during the disposition of alerts.

3.7. Obligations of Designated Director

- The Designated Director shall bear overall responsibility for the effective implementation and oversight of the surveillance framework of the Broking Division.
- They shall ensure that adequate resources, systems, and controls are in place to monitor and detect abnormal or suspicious trading activities.
- The Designated Director shall periodically review the MIS reports submitted by the Compliance Officer, evaluate the action taken on alerts, and provide necessary guidance or directives for strengthening the surveillance process where required.
- It shall be the duty of the Designated Director to ensure that surveillance-related responsibilities are discharged in line with the applicable laws, rules, and regulatory expectations.

3.8. Obligations of Internal Auditor

- The Internal Auditor of the trading member shall be responsible for conducting an independent review of the Surveillance Policy, including its adequacy, implementation, and operational effectiveness.
- As part of the audit, the Internal Auditor shall verify whether the surveillance alerts—both from exchanges and those generated internally—are being properly reviewed, investigated, and acted upon as per defined procedures.
- The auditor shall assess:
 - a. The timeliness and appropriateness of responses to surveillance alerts;
 - b. The documentation and escalation process;
 - c. The adequacy of records maintained;
 - d. The overall compliance with internal policies and external regulatory norms.
- All observations, findings, and recommendations related to the surveillance framework shall be duly documented in the Internal Audit Report, which shall be submitted to the management and Designated Director for review and corrective action, if necessary.

3.9. Obligation of Quarterly reporting of status of the alerts generated by broking

division:

- Broking division is also required to provide duly approved status of the alerts on a quarterly basis, in the following format to the Exchange within 15 days from end of the quarter.

Name of Alert	Number of alerts under process at the beginning of quarter	Number of new alerts generated in the quarter	Number of alerts Verified and closed in the quarter	Number of alerts referred to Exchange	Number of alerts pending/ under process at the end of quarter
	(A)	(B)	(C)	(C1)	[(D) = (A)+(B)-(C)]

(*) Details of alerts referred to the Exchange:

Sr. No.	Date of Alert	Type of Alert	Brief observation and details of action taken	Date referred to Exchange

Details of any major surveillance action taken (other than alerts referred to Exchange), if any, during the quarter:

Sr. No.	Brief action taken during the quarter

- If Broking division does not have anything to report, it will submit 'NIL Report' within 15 days from end of the quarter.

4. ESCALATION AND REPORTING MECHANISMS
4.1. Apex Body Oversight & Quarterly MIS

- The Apex Body (Audit Committee / Board of Directors / equivalent governing body) shall review compliance with the surveillance framework at least once every quarter.
- The review shall include adequacy of internal controls, surveillance system effectiveness, reporting quality, deviations, and corrective measures.

- A Quarterly MIS covering alerts, escalations, client exceptions, and filings shall be submitted every quarter.

4.2. Reporting of Suspicious Activity Within 48 Hours

- Upon detection of any suspicious activity, Trading Members shall inform the Stock Exchanges as soon as reasonably possible, but not later than 48 hours from detection.
- Reporting may be via email or Member Surveillance Dashboard (MSD).
- Details reported shall include client information, alert description, observed patterns, and preliminary analysis.

4.3. Reporting of Deviations & Internal Escalation

- Deviations from internal controls, RMS, Surveillance Policy, and Client Onboarding processes must be placed before the Committee / Board at regular intervals.
- Such deviations shall be included in statutory submissions to the Exchanges.
- The PO / DD / CO / CSO shall report deviations to the Apex Body and Stock Exchanges.

4.4. Seeking Guidance from Stock Exchanges

- If suspicious activity is detected but violation of law cannot be established due to lack of information, Trading Members shall seek guidance from Exchanges.
- All such suspicious activity must still be communicated as per NSE Circular NSE/SURV/44477 dated May 27, 2020.

4.5. Accountability Grid for Suspicious Behaviour

Who is Being Surveilled	Primary Responsibility for Trade Surveillance	Escalation / Review Authority
Clients	Surveillance Team under supervision of Senior Management; Compliance Officer; Designated Director; CEO	CEO/ Executive Director/ Board-level Committee (Surveillance/ Audit Committee)
Authorised Persons (APs)	Surveillance Team + Compliance Officer + Senior Management	CEO/ Executive Director/ Board-level Committee

Employees (including dealing staff)	Senior Management; Key Managerial Personnel (KMP); Designated Director (<i>Designated Director refers to the Director designated under SEBI/PMLA framework for AML & Surveillance oversight</i>); Compliance Officer	Board of Directors/ Audit Committee
Promoters	Board of Directors/ Audit Committee	Full Board (excluding interested directors)
CEO/ Executive Director/ Senior Management/ KMP	Board of Directors/ Audit Committee	Board of Directors (Independent Oversight)
Related Accounts/ Connected Entities/ Relatives	Surveillance Team + Compliance	Senior Management + CEO
Algo Users	Algo Surveillance Team/ IT & Surveillance	Senior Management/ Compliance + CEO
Dormant/ High-Risk Accounts	Surveillance Team	Senior Management + Compliance Head

5. GENERAL PROVISIONS

5.1. Applicability, Compliance, and Policy Implementation

- The Compliance Team shall ensure adherence to the latest regulatory circulars issued by SEBI, Exchanges, and Depositories.
- All employees are required to strictly adhere to the obligations, procedures, and timeframes defined under this Policy.

5.2. Management Discretion and Policy Flexibility

The Company acknowledges that surveillance requirements are subject to evolving regulatory standards issued by SEBI, Exchanges, Depositories, and other competent authorities. The Management reserves the right to revise or amend this Surveillance Policy, in whole or in part, to ensure continued compliance with such regulatory developments. Accordingly, this Policy shall remain flexible and may be updated from time to time based on Management's perception of risk, emerging trends, or directives from regulatory bodies. Such changes, when made, shall be properly documented and communicated to relevant stakeholders.

5.3. Interpretation of Terminology and Policy Applicability

Wherever the terms "Company ", "Trading Member", "Stock Broker", "Depository Participant", "Broking Division" (referring to the stock broking operations of the Company),

"DP Division" (referring to the depository participant operations of the Company), or "Member" are used in this Policy, they shall be deemed to refer to Unique Stockbro Private Limited in its capacity as a registered Trading Member of the National Stock Exchange of India Limited (NSE) and BSE Limited (BSE), and as a Depository Participant with Central Depository Services (India) Limited (CDSL).

For & behalf of
Unique Stockbro Private Limited

Compliance Officer
Broking Division

Compliance Officer
DP Division

Date: January 13, 2025

End of Report

Disclaimer: The Surveillance Policy as outlined above is subject to change from time to time, based on evolving circumstances and applicable regulatory guidelines. The Surveillance Policy will be reviewed periodically in line with regulatory requirements and management's assessment.

Standard Operating Procedure (SOP) for Surveillance Policy Implementation
Unique Stockbro Private Limited

1. Objective

To lay down a structured operational framework for effective implementation and monitoring of the Surveillance Policy across all divisions of Unique Stockbro Pvt. Ltd., ensuring strict adherence to applicable regulatory guidelines issued by SEBI, CDSL, NSE, BSE, and any other competent authority.

2. Scope

This SOP applies to both the Depository Participant (DP) and Broking Divisions of the Company. It covers procedures related to:

- a. Alerts generated internally by the DP or Broking Division, its review and its closure
- b. Alerts downloaded from CDSL (DP Alerts), its review and its closure
- c. Alerts downloaded from NSE/ BSE (Broking Alerts), its review and its closure
- d. Client due diligence and escalation
- e. Regulatory reporting and MIS generation
- f. Record-keeping and audit mechanisms

3. Responsibility Matrix

Designation	Responsibility Description
Surveillance Team	Daily alert monitoring, analysis, MIS preparation
Compliance Officer	Oversight, regulatory reporting, escalation, coordination with auditors and authorities
Designated Director	Strategic oversight, periodic MIS review, promotion of surveillance culture
Internal / Concurrent Auditor	Independent validation of surveillance processes and controls

4. Operating Procedures (DP & Broking Division)**4.1. Daily Surveillance & Alert generation Parameters**

Surveillance alerts and themes shall be generated from multiple sources, including (i) downloaded alerts from the CDSL Surveillance Portal, (ii) Member Surveillance Dashboards of NSE and BSE, and (iii) alerts triggered through internal surveillance systems. The Surveillance Team shall monitor and analyse all alerts and transactions falling under various risk categories as defined in the Surveillance Policy. Further, considering the dynamic nature of the securities

market, emerging trading patterns, and evolving risk indicators, the Surveillance Team shall remain vigilant, continuously observe market behaviour, and analyse any unusual or suspicious activity even if it does not fall within the predefined alert categories

4.2. Alert Analysis and Documentation

Evaluate alerts with supporting documentation (demat statements, KYC, financials, transaction history).

Document findings and record outcome in an Alert Register:

Field	Description
Date of Generation	Date of alert trigger
Nature of Alert	Off-market / pledge / etc
Status	Pending / Closed / Escalated
Remarks	Reason for closure or escalation rationale

4.3. Timelines for Processing Alerts

Alert Type	Response Timeline	Remarks
CDSL Alerts (DP)	30 calendar days	Final status must be updated on CDSL system
Internal DP Alerts with adverse findings	Within 7 calendar days	Must be reported to CDSL
NSE/BSE Alerts	Within 45 calendar days	Final status to be updated on the Exchange portal
Internal Broking Alerts with adverse findings	Within 90 calendar days	Must be reported to Exchange

4.4. Escalation Protocol

Escalate serious irregularities to the Compliance Officer. If warranted, Compliance Officer shall escalate the matter to CDSL or FIU-IND.

Escalation Level	Trigger	Action
Surveillance Team → Compliance Officer	Any suspicious or abnormal client activity	Document and raise for review
Compliance Officer → CDSL/NSE/BSE/FIU-IND	Confirmed suspicious activity or PMLA red flags	Report with all supporting documents
Compliance Officer → Designated Director	Repeated violations, systemic risk concerns	Included in Quarterly MIS with recommendations
Internal Auditor → Management	Audit findings or process lapses	Suggest process improvement or disciplinary action

4.5. Quarterly MIS

- Prepare and submit the Quarterly MIS for the DP Segment (as per Section 2.9 of the Policy) and for the Broking Division – CM Segment (as per Section 3.9 of the Policy) to the Compliance Officer within 10 days from end of quarter.
- Compliance Officer to present to Designated Director for review.

5. Client Due Diligence (CDD)

- Continuous review of KYC, income proofs, transactional patterns.
- Group clients by PAN / Email/ Phone to identify group trading or coordinated activity.

6. Record Maintenance (for all verticals)

Retain all supporting documents (communication trail, investigation records, closure notes) for minimum 5 years.

- Maintain both electronic and hard copy records for minimum 5 years or as required under PMLA, whichever is higher.
- Maintain indexed registers with:
 - Alert ID
 - Client Code
 - Alert Date
 - Disposition Date
 - Closure Reason or Escalation Note
 - Supporting Evidence Reference

7. Compliance Officer Duties

- Ensure end-to-end adherence to surveillance SOPs across divisions.
- Scrutinize MIS and alerts under closure/escalation categories.
- Interface with regulatory bodies and submit necessary reports.
- Conduct annual training for the surveillance team.
- Facilitate audits and respond to observations in a time-bound manner.

8. Designated Director Responsibilities

- Conduct bi-annual reviews of Surveillance MIS.
- Monitor systemic risks and recommend policy enhancements.

- Promote ethical standards and surveillance-driven compliance culture.

9. Obligations of Internal Auditor / Concurrent Auditor

- Periodic review of surveillance records and alert handling timelines.
- Assess effectiveness of closure rationale and escalation triggers.
- Submit audit report to the Compliance Officer and Designated Director.
- Highlight gaps and suggest systemic improvements.

10. Review and Amendment of SOP

SOP to be reviewed annually or upon material regulatory change, whichever is earlier. All updates to be approved by the Board of Directors and communicated to stakeholders.

For & behalf of
Unique Stockbro Private Limited

Compliance Officer
Broking Division

Compliance Officer
DP Division

Date: January 13, 2025

End of Report

Disclaimer: *The Surveillance Policy and Standard Operating Procedure (SOP) outlined above are subject to change from time to time, based on evolving circumstances and applicable regulatory guidelines. The Surveillance Policy will be reviewed periodically in line with regulatory requirements and management's assessment.*