Allvest Securities Private Limited

SURVEILLANCE & MONITORING POLICY

Document Revision and Version Control

Version no	Month	Prepared by	Reviewed by	Adopted in Board
Ver 1	Feb 2026	Kandarp Padh	Amit Bansal	23/02/2026

CONTENTS

INTRODUCTION 3

FRAMING OF THE SURVEILLANCE POLICY 3

OBJECTIVE 5

SCOPE OF THE POLICY 5

OBLIGATION TO GENERATE ADDITIONAL SURVEILLANCE ALERTS RELATING TO STOCK BROKING OPERATIONS 6

OBLIGATION TO GENERATE ADDITIONAL SURVEILLANCE ALERTS RELATING TO DEPOSITORY OPERATIONS 8

OBLIGATION FOR REPORTING THE STATUS OF ALERTS GENERATED FOR DEPOSITORY SERVICES 10

OBLIGATION WITH RESPECT TO CLIENT DUE DILIGENCE 11

OBLIGATION WITH RESPECT TO PROCESSING OF ALERTS 12

RESPONSIBILITIES OF COMPLIANCE OFFICER, DESIGNATED DIRECTORS, AND INTERNAL AUDITOR/CONCURRENT AUDITOR 13

OBLIGATION OF QUARTERLY REPORTING OF STATUS OF THE ALERTS GENERATED 14

REVIEW OF THE POLICY AND UPDATE 15

INTRODUCTION

Allvest Securities Private Limited (hereinafter referred to as "ASPL" or "Company") is incorporated under the Companies Act, 2013, with Corporate Identification Number (CIN) U66120MH2025PTC440678. ASPL is registered as Stock Broker with SEBI having Registration number INZ000330839 and is registered as Trading Cum Self Clearing Member with National Stock Exchange of India Ltd and NSE Clearing Ltd. (Member Code: 90469), as a Trading Member with BSE Ltd. (Member Code:6973), as a Trading Cum Self Clearing Member with Multi Commodity Exchange of India Limited (Member Code :57650) and ASPL is also registered with SEBI as a Depository Participant having Registration No.: IN-DP-837-2026 and with NSDL having DP ID: IN304949. It is registered with AMFI with registration number 346229.

FRAMING OF THE SURVEILLANCE POLICY

Allvest, as a Stock Broker and Depository Participant, recognizes its obligation to establish a robust Surveillance Policy to ensure the integrity of the securities market. This policy is designed to:

- Establish a framework to generate surveillance alerts, considering both internal parameters and transactional alerts downloaded by the Exchange.
- Define risk-based thresholds to identify suspicious trading patterns based on client activity and market trends.
- Mandate that all alerts—whether Exchange-generated or internally identified—are processed within 45 days from the date of their generation.
- Ensure that any delay in alert disposition is duly documented with valid reasons to maintain transparency and accountability.
- Establish mechanisms to detect and flag potential manipulative or fraudulent activities, such as circular trading, price rigging, and front running.
- Define measures for dealing with suspect clients, including suspension of trading activities or other disciplinary actions as per regulatory requirements.
- Comply with obligations under the Prevention of Money Laundering Act (PMLA) to prevent illicit activities.
- Ensure that all surveillance-related records are maintained as per statutory guidelines to facilitate audits and regulatory compliance.
- Review and dispose of transactional alerts provided by NSDL, which are based on defined thresholds. DPs may establish additional parameters to detect suspicious transaction activity.
- Ensure disposal of alerts within 45 days from the date of generation, whether provided by NSDL or generated internally.
- Report abnormal activities to NSDL and other relevant authorities as applicable.
- Maintain documentation for any delay in alert disposition.
- Define a framework for appropriate actions under PMLA obligations.
- Conduct an annual review of the surveillance policy to ensure alignment with regulatory and market developments.

In addition to the obligations mentioned above, Allvest is required to:

- Prepare a Standard Operating Procedure (SOP) for processing surveillance alerts, which includes alerts generated at Allvest's end as well as alerts generated by NSDL.
- Ensure that the SOP includes alert generation parameters, establishes timelines for response, outlines escalation procedures, and defines any other essential processes related to alert handling.
- Review the SOP and alert parameters on a periodic basis, with oversight by the Compliance Officer.
- Ensure that a Maker-Checker mechanism is followed during the processing and disposal of surveillance alerts.

1. **Policy Design**

   Allvest shall frame its surveillance policy keeping in view the nature of its depository business, client profile, volume of demat accounts, and transaction patterns. The policy shall be a living document, updated in line with regulatory developments.

2. **Core Requirements**

   a. **Alert Generation** Allvest shall generate surveillance alerts suited to its business profile, guided by (but not limited to) indicative themes prescribed by NSDL. Additional internally defined parameters and thresholds may be adopted to detect abnormal activity more effectively.

   b. **Review of NSDL Alerts** Alerts provided by NSDL (based on prescribed thresholds) shall be reviewed systematically alongside internally generated alerts, which may operate on different or more granular parameters.

   c. **Alert Disposal Timeline** All alerts — internal or NSDL-provided — shall be disposed of within 45 days of generation. Reasons for any delay shall be documented and maintained on record.

   d. **Reporting Obligations** Any abnormal or suspicious activity identified through the alert review process shall be reported to NSDL and other applicable authorities as required.

   e. **PMLA Framework** The policy shall incorporate a clear framework of actions available to Allvest as a Depository Participant under the Prevention of Money Laundering Act (PMLA).

   f. **Record Retention** All surveillance records shall be retained for the periods prescribed under applicable statutes.

3. **Operational & Governance Requirements**

   a. **SOPs** A comprehensive SOP shall be maintained, drawing from the surveillance policy, SEBI regulations, NSDL circulars, and internal systems, serving as the day-to-day operational reference.

b. **SOP Approval** A defined approval mechanism shall govern adoption and revision of SOPs before implementation.
c. **Regulatory-Triggered Reviews** The policy shall be reviewed beyond the annual cycle whenever warranted by changes in SEBI regulations, NSDL circulars, or material changes in business operations.
d. **Maker-Checker & Segregation of Duties** Alert approvals, reporting, and escalation activities shall follow a maker-checker mechanism with clear segregation of duties to ensure independence and accountability.
e. **Resource Adequacy** The surveillance function shall be supported by suitably qualified and trained personnel, along with adequate systems and technology.
f. **Alert Parameter Review** Existing alert parameters shall be periodically evaluated and revised where found inadequate or outdated.
g. **New Alert Introduction** A process shall exist to introduce new alert types based on risks and patterns identified through day-to-day operations.
h. **Staff Training** Personnel involved in surveillance shall undergo periodic training covering regulatory requirements, internal procedures, and emerging risk typologies.

OBJECTIVE

The objective of this policy is to:

- Develop parameters to generate alerts and / or reports for identifying suspicious or potentially manipulative transactions.
- Monitor alerts generated.
- Report suspicious / manipulative activities as required by SEBI/Exchanges/NSDL.
- Minimize business risk through better profiling of clients based on monitoring and surveillance of transactions.

SCOPE OF THE POLICY

This Policy requires Allvest to review surveillance alerts provided by the Exchange(s)/NSDL
The review of Exchange(s)/NSDL alerts includes -

- Preliminary assessment of alerts.
- Connecting with clients for clarification, if required
- Internal discussion with concerned teams/ trader for further deliberation (if required)
- Disposing the alerts in timely manner.
- Escalation of adverse findings/comments with Stock Exchanges within a prescribed time frame.
- Allvest will continue to review this policy as and when alerts categories are amended /added by the Exchanges/NSDL/SEBI internal parameters, appropriately.

OBLIGATION TO GENERATE ADDITIONAL SURVEILLANCE ALERTS RELATING TO STOCK BROKING OPERATIONS

Allvest, as a Stock Broker and Depository Participant, is committed to implementing a robust Surveillance Framework to ensure the effective monitoring of client trading activities. In addition to transactional alerts downloaded by the Exchange, Allvest is obligated to generate its own surveillance alerts in line with its business model, client base, and regulatory expectations.

This policy outlines the indicative themes for surveillance alerts, ensuring the detection of any unusual or suspicious trading patterns.

The transactional alerts provided by the Exchange are as follows (Indicative in nature):

Sr. No.	**Transactional Alert**	**Segment**
1.	Significant increase in client activity	Cash
2.	Sudden trading activity in dormant account	Cash
3.	Clients/Group of Client(s), dealing in common scrips	Cash
4.	Client(s)/Group of Client(s) concentrated in few illiquid scrips	Cash
5.	Client(s)/Group of Client(s) dealing in scrip in minimum lot size	Cash
6.	Client / Group of Client(s) Concentration in a scrip	Cash
7.	Circular Trading	Cash
8.	Pump and Dump (Pump-and-dump" involve the touting of a company's stock (typically small, so-called "microcap" companies) through false and misleading statements to the marketplace.)	Cash
9.	Wash Sales	Cash & Derivatives
10.	Reversal of Trades	Cash & Derivatives
11.	Front Running (i.e. Execution of orders in a security for its own account by the member while taking advantage of advance knowledge of orders from its customers)	Cash
12.	Concentrated position in the Open Interest / High Turnover concentration	Derivatives
13.	Order book spoofing i.e. large orders away from market	Cash

Allvest shall regularly download alerts from BSE and NSE portals including Exchange Surveillance Dashboard, conduct a thorough review and analysis, and ensure their timely closure

Obligation to Generate Additional Surveillance Alerts

Allvest shall proactively generate internal surveillance alerts to effectively monitor client trading activities in accordance with its Surveillance Policy. This involves:

- Identifying suspicious patterns and trends in trading behavior.
- Ensuring risk-based monitoring for potential market manipulation.
- Taking appropriate actions where necessary, including escalation to regulators if required.

Indicative Themes for Surveillance Alerts

Allvest shall analyze trading patterns and generate alerts based on the following indicative themes:

Themes Applicable to All Clients

High Concentration in Trading Activity

- Clients or a group of clients accounting for a significant percentage of the total trading volume in a particular scrip/contract as compared to market trends.

New or Dormant Clients with High Trading Activity

- Clients with newly opened accounts or those resuming trading after a long gap, exhibiting high-value transactions in specific scrips/contracts.

Frequent Small-Lot Trading

- Clients placing frequent small-quantity or minimum market lot trades in a specific scrip/contract, potentially indicating layering or manipulation.

Disproportionate Trading vs. Financial Profile

- Clients executing transactions inconsistent with their reported income or net worth, raising concerns about possible funding from undisclosed sources.

Frequent KYC Modifications

- Clients who frequently change KYC details such as address, phone number, or bank account details, possibly to evade surveillance.

Trading Prior to Price-Sensitive Announcements

- Clients who trade in securities before price-sensitive announcements by a listed company, potentially having direct or indirect connections to the entity.

High Selling Concentration in Monitored Scrips

- Clients with significant selling positions in scrips under the Exchange's 'For Information List' or 'Current Watch List', requiring enhanced monitoring.

Consistent Profit/Loss Patterns

- Clients or groups of clients consistently making profits or losses, necessitating a review of the rationale and legitimacy of trading strategies.

Trading in Pledged Securities

- Clients engaging in significant trading in securities they have pledged, which may indicate financial distress or circular trading.

Verification of Client Order Placement

- In case of concerns regarding a client's trading activity, ensuring that orders are being placed by the actual client or an authorized representative.

- Monitoring client address in KYC vs. dealing office address to detect potential unauthorized trading activities.

Additional Themes for Depository Participants
For clients using Allvest's Depository Participant services, the following additional alerts shall be monitored:

Trading in Pledged or Significant Holdings
- Clients executing significant trades in securities they have pledged or where they have frequent off-market transactions, warranting enhanced scrutiny.

Additional Themes for Internet-Based Trading Clients
For clients using Allvest's Internet-Based Trading Platform, the following additional monitoring measures shall be implemented:
- Monitoring and identifying instances of multiple client codes trading from the same IP address or unusual geographic locations to detect potential misuse or unauthorized access.

Independent Judgment and Customization of Alerts
The above themes serve as illustrative guidelines and are not exhaustive. Allvest shall, based on its business model, client profile, and regulatory requirements, exercise its independent judgment to:
- Formulate additional customized surveillance alerts where necessary.
- Conduct ongoing analysis of evolving market trends.
- Take appropriate action in case of suspicious trading activity, including reporting to regulatory authorities if required.

OBLIGATION TO GENERATE ADDITIONAL SURVEILLANCE ALERTS RELATING TO DEPOSITORY OPERATIONS

Allvest, as a Depository Participant (DP) of NSDL, is required to generate appropriate surveillance alerts to effectively monitor the transactions of its clients as per the laid-down surveillance policy. The indicative themes on which Allvest may formulate its own alerts are outlined below. Additionally, Allvest must analyze patterns and trends with respect to different themes.

(Part A)

Sr. No.	Indicative Theme
1	**Alert for multiple demat accounts opened with identical demographic details:** Accounts opened with the same PAN, mobile number, email ID, bank account number, or address, considering the existing demat accounts held with Allvest.
2	**Alert for communication failures:** Emails or letters sent to the registered email ID or address of clients getting bounced.
3	**Frequent changes in account details:** Repeated modifications in details such as address, email ID, mobile number, authorized signatory, and POA holder.
4	Frequent off-market transfers by a client within a specified period.
5	Off-market transfers not commensurate with the client's declared income/networth
6	Pledge transactions that are inconsistent with the client's income/net worth.
7	High-value off-market transfers immediately following modifications in account details
8	**Review of off-market transfers and their stated reasons:** Transfers categorized as gifts with consideration, frequent transfers to unrelated parties, and frequent transfers with the reason code "off-market sales" that do not align with the client's profile
9	**Alert for newly opened accounts with unusual transaction patterns:** Sudden spikes in trading activity followed by a sharp drop in holdings, leading to dormancy.
10	Any other alerts or mechanisms necessary to detect and prevent market manipulation by clients.

Part B

Sr. No.	Additional Indicative themes:
1	Off-market transfer of securities from one demat account to many demat accounts without any economic rationale.
2	Off-market receipt of securities from multiple demat accounts to one demat account without any economic rationale.
3	Multiple demat accounts opened with noticeably short / incomplete address.
4	Different demat accounts of same persons with different PANs.
5	Demat accounts of a person used by another person for deceptive purposed.
6	Multiple off-market transfers (value and volume based) with potentially incorrect off- market reason code declared.

7	Shifting of ownership of securities to avoid attachment of securities by government authorities or under IBC / NCLT.
8	Fraudulent / unauthorised transfers in dormant demat accounts.

The above-mentioned alerts will be generated based on predefined thresholds and parameters. These alerts are illustrative and not exhaustive. Allvest must analyze and review these alerts based on factual data and verification of relevant documents, including income and net worth as provided by the Beneficial Owner (BO). Furthermore, Allvest shall exercise independent judgment and take appropriate action to detect and mitigate any abnormal or suspicious transactions.

All the alerts will be analysed in detail by taking into consideration the current and historical trade data, order data, financial details of the client, KYC details of the client, security group, nature of the scrip like liquid or illiquid, price movement in the scrip etc. & other relevant documentary evidences.

In case of Suspicion, trading rationale and necessary documentary evidences including bank statements, demat statements, Income Proofs etc. will be sought from the client & after analysing the documentary evidences, the comments will be recorded for the alerts & thereafter, such alerts are either disposed-off in case of no concern observed or reported to FIU-India &/or NSE, BSE, NSDL as the case may be.

Once the Suspicion is established, the case will be discussed among Surveillance Head, Compliance Officer and Principal Officer. The STRs will be filed based on email approval from the Principal Officer.

STRs will be filed within 7 days from date of approval received from the Principal Officer.

OBLIGATION FOR REPORTING THE STATUS OF ALERTS GENERATED FOR DEPOSITORY SERVICES

- Allvest is required to maintain a register (electronic/physical) for recording all alerts generated.
- While reviewing alerts, Allvest shall obtain transaction rationale, verify demat statements, and obtain supporting documents as required from the client.
- After verifying the documentary evidence, Allvest will record its observations for such identified transactions of its clients.
- With respect to the transactional alerts provided by NSDL, Allvest shall ensure that all alerts are reviewed, and their status (Verified & Closed / Verified & Reported to NSDL), including action taken, is updated within 45 days. A detailed procedure regarding the

sharing of alerts by NSDL with Allvest and report submission in this regard will be provided separately.

With respect to the alerts generated at Allvest's end, instances with adverse observations, along with details of the action taken, shall be reported to NSDL within 7 days from the date of identification of the adverse observation.

OBLIGATION WITH RESPECT TO CLIENT DUE DILIGENCE

Allvest is committed to implementing a comprehensive Client Due Diligence (CDD) framework to ensure regulatory compliance and mitigate risks associated with financial transactions. This policy outlines the obligations of Allvest in conducting ongoing due diligence, periodic KYC updates, and client association analysis.

Ongoing Client Due Diligence

Allvest shall conduct continuous due diligence on all its clients to ensure that their trading and investment activities remain consistent with their declared financial profiles, risk tolerance, and regulatory requirements.

Periodic KYC Updates

Allvest shall:

- Ensure that key KYC parameters of clients are updated periodically as per SEBI regulations.
- Maintain and update the latest client information in the Unique Client Code (UCC) database of the Exchange.
- Verify that the client's identity, address, and financial details remain accurate and in compliance with regulatory norms.

Identification of Client Associations & Common Accounts

Allvest shall analyze available client data to:

- Identify multiple accounts linked to the same individual or entity.
- Detect common accounts or group associations among clients based on shared credentials such as:
    - Common mobile numbers, email addresses, or addresses.
    - Common bank accounts or demat accounts.
    - Trading patterns indicative of potential collusion or market abuse.

Compliance and Risk Mitigation

- Allvest shall ensure that any discrepancies or suspicious activities identified through due diligence are escalated for further review.

- In case of any regulatory breaches, necessary actions, including reporting to the authorities and potential client account restrictions, shall be taken.

OBLIGATION WITH RESPECT TO PROCESSING OF ALERTS

Processing of Alerts

Collection of Trading Rationale and Supporting Documents

Allvest shall:

- Obtain the trading rationale from clients for transactions flagged in alerts.
- Collect necessary supporting documents, including:
    - Bank statements to verify the flow of funds.
    - Demat statements to verify securities transactions and holdings.
    - Any other relevant records required for investigation.

Documentation and Recording of Observations

- After analyzing the gathered evidence, Allvest shall:
    - Document its observations regarding the identified transactions.
    - Maintain a clear audit trail of the analysis, findings, and conclusions drawn from the review.

Processing of Exchange-Generated Alerts

- For transactional alerts downloaded by the Exchange, Allvest shall:
    - Ensure that each alert is thoroughly analyzed.
    - Update the status of each alert as "Verified & Closed" or "Verified & Sent to Exchange" based on the findings.
    - Complete this process within 45 days from the date of alert generation.
    - Update the action taken in the Member Surveillance Dashboard.

Processing of Internal Alerts & Reporting to Exchange

- For alerts generated internally by Allvest, the following measures shall be taken:
    - Review and analyze the alerts to determine if there are adverse observations.
    - If any suspicious or non-compliant activity is detected, Allvest shall:
        - Take appropriate action against the concerned client.
        - Report the instance to the Exchange within 45 days from the date of alert generation, along with details of the action taken.

4. Surveillance Obligations – Processing of Alerts for Depository operations

Part A

- Allvest shall maintain a register (electronic/physical) for recording all alerts generated.
- While reviewing alerts, Allvest shall obtain the transaction rationale, verify the demat account statement, and obtain supporting documents from the client, wherever required.
- Upon verification of documentary evidence, Allvest shall record its observations for the identified transactions of the client.

- With respect to transactional alerts received from NSDL, Allvest shall ensure that all alerts are reviewed and the status thereof (Verified & Closed / Verified & Reported to NSDL), along with action taken, is updated within 45 days on the NSDL e-PASS portal.
- With respect to alerts generated at Allvest's end, instances involving adverse observations shall be reported to NSDL, along with details of action taken, within 7 days from the date of identification of such adverse observation, through the NSDL e-PASS portal.

Part B

- Allvest shall refer to alert-wise guidelines available on the NSDL e-PASS portal while reviewing alerts.
- Allvest shall adhere to the prescribed guidelines in letter and spirit to ensure timely, complete, and accurate resolution of alerts, avoiding any rejection of responses submitted.
- Allvest shall maintain and provide supporting documents, wherever necessary, to substantiate responses, including but not limited to account opening forms, client correspondence, and internal investigation reports.

RESPONSIBILITIES OF COMPLIANCE OFFICER, DESIGNATED DIRECTORS, AND INTERNAL AUDITOR/CONCURRENT AUDITOR

Compliance Officer's Role

- The surveillance activities of Allvest shall be conducted under the overall supervision of the Compliance Officer.
- The compliance officer to ensure timely generation and disposal of internal surveillance alerts.
- The compliance officer of the Depository Participant shall ensure the quality of responses for closure of alerts using sampling method, in terms of completeness.
- The compliance officer and internal auditor may provide their suggestions to improve the overall quality and effectiveness of surveillance operations, where necessary.

Reporting to Designated Directors

- A quarterly MIS report shall be submitted to the Designated Directors including:
    - Number of alerts pending at the start of the quarter.
    - Number of new alerts generated during the quarter.
    - Number of alerts processed and acted upon during the quarter.
    - Number of alerts pending at the end of the quarter, along with reasons for pendency and an action plan for closure.
    - Any exceptions noticed during alert disposition.

Accountability of Designated Directors

- The Designated Directors shall be responsible for all surveillance activities carried out by Allvest.

Internal/Concurrent Auditor's Role

- The Internal Auditor shall:
  - Review the surveillance policy, its implementation, and effectiveness.
  - Examine the alerts generated during the audit period.
  - Record observations in the audit report.
  - Internal Auditor shall verify that the quarterly MIS is prepared and placed before the Board of the Depository Participant.

Generation and Analysis of Alerts, Obtaining Information, Collecting Documentary Evidences and Filing of STRs

- In order to comply with the above-mentioned Exchange and Depository requirements for the Surveillance purpose, ASPL will deploy the Surveillance tool viz. Trackwizz which has a different kind of alert scenarios in order to generate alerts based on the threshold set for every different type of alert.
- The alerts provided by NSE, BSE and transactional alerts provided by NSDL shall be processed into Trackwizz.
- All Internal alerts in line with the NSE, BSE and NSDL indicative themes will be generated on T+1 basis.
- All the alerts provided by the NSE, BSE and generated internally will be disposed off within 45 days from the date of alerts downloaded from the member portal such as e-Boss and e-NIT and generated internally.
- All alerts provided by NSE & BSE will be analysed and status thereof such as Verified & Closed / Verified & Sent to Exchange including action taken will be updated within 45 days, in the e-BOSS & e-NIT portal.
- All alerts provided by NSDL and generated internally will be disposed-off within 30 days from the date of alerts downloaded from the participant's portal and generated at participant's end.

OBLIGATION OF QUARTERLY REPORTING OF STATUS OF THE ALERTS GENERATED

Allvest shall submit a quarterly report to NSDL in the following format within 15 days from the end of the quarter:

A. Status of Alerts Generated by Allvest for stock broking operations

Name of Alert	Alerts under process at the start of the quarter	New alerts generated	Alerts Verified & Closed	Alerts referred to Exchange	Alerts pending at the end of the quarter

B. **Alerts Referred to Exchange**

Sr. No.	Date of Alert	Type of Alert	Brief Observation & Action Taken	Date Referred to Exchange

C. **Details of Major Surveillance Actions Taken (Other than Alerts Referred to Exchange)**

Sr. No.	Brief Action Taken

D. **Status of Alerts generated by Allvest for Depository operations:**

Name of Alert [A]	No. of alerts pending at beginning of quarter [B]	No. of new alerts generated during the quarter [C]	No. of alerts Verified s closed in the quarter [D]	No. of alerts reported to Depository [E]	No. of alerts pending for process at the end of quarter (If any) [F] = [B+C]-[D+E]	Ageing analysis of the alerts pending at the end of the Quarter (since alert generation date) (Segregation of F column)					Reason for pendency
						< 1 month	1-2 months	2-3 months	3-6 months	> 6 months	

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

Sr. No.	Brief action taken during the quarter

b. Allvest shall submit a 'NIL Report' within 15 days from end of the quarter if there are no alerts generated for a particular quarter.

c. The above details shall be uploaded by Allvest on NSDL e-PASS Portal.

Uploading Reports

- The above details shall be uploaded on the respective portal or as communicated by Exchanges/NSDL from time to time within 15 days from the end of the quarter.

REVIEW OF THE POLICY AND UPDATE

The policy will be reviewed and updated as required to incorporate any changes introduced by regulatory authorities. Additionally, it will undergo periodic review at least once in a year to ensure its continued relevance, effectiveness, and alignment with current regulatory requirements and industry standards by the Board.