FAIR INTERMEDIATE INVESTMENT PVT. LTD.

SURVEILLANCE ALERT POLICIES AND PROCEDURES,MONITORING & DISPOSITION OF ALERTS FOR BROKING AND DEPOSITARY PARTICIPANT OPERATIONS

Dated 05.11.2025

Applicability and Objective

This policy applies to the stock broking (NSE, BSE, MCX) and Depository Participant (CDSL) operations of Fair Intermediate Investment Pvt. Ltd. Its primary objective is to establish a robust monitoring system to detect, analyze, and report suspicious trading patterns or transactions that may involve market manipulation, insider trading, or money laundering.

This policy has been formulated and updated in accordance with the key points outlined below:

1. **SEBI (Stock Brokers) Regulations, 2026**: Mandating the establishment of internal controls for brokers to detect and report fraud or market abuse.
2. **SEBI Master Circular on Surveillance (July 2024/2025):** Consolidating all surveillance-related obligations for market intermediaries.
3. **PMLA (Maintenance of Records) Rules, 2005:** Governing the reporting of Suspicious Transaction Reports (STRs).
4. **Exchange and Depository Circulars:** Including NSE/SURV/48818 and CDSL/OPS/DP/SYSTM/2021/309, pertaining to transactional alert monitoring.

Background:

Surveillance is the process of collecting and analyzing information concerning markets in order to detect unfair transactions that may violate securities related laws, rules and regulations. Trading Members & Depository Participants have the responsibility of monitoring the trading activity of their clients. Trading Members have been advised by the Stock Exchanges, Depository & extant Regulators to set-up monitoring of the Trading Activity and Movement of securities of their clients including intra-day activity and proactively report to the Exchanges/ Depository/ Extant Regulators observations/ findings, if any. In order to achieve this and to create safer markets, an adequate surveillance policies and system to be put in place in order to monitor suspicious/ manipulative transactions and curb such activities, if any.

Sources of Surveillance Alerts

The entity shall monitor and process alerts from three primary sources:

- Exchanges/Depository Provided Alerts: Alerts downloaded from the surveillance portals of NSE, BSE, MCX, and CDSL.
- Internal Surveillance Mechanism: System-generated alerts based on predefined criteria such as sudden volume spurts, price manipulation, or "circular trading" patterns.
- Regulatory Intimations: Direct alerts or queries received from SEBI or other regulatory bodies.

Resolution and Processing Timelines

1. **Internal Analysis:** All alerts (whether generated internally or provided by the Exchange) are analyzed by the Compliance/Surveillance Team. In the case of complex alerts, they may be kept "under surveillance" for up to 15 days.
2. **Closure Timeline:** Alerts are processed and closed within 45 days of their generation (or download from the Exchange).
3. **Adverse Observations:** If an alert remains suspicious even after due investigation, it is reported to the concerned Exchange/Depository within 7 days of identifying the adverse observation.

Implementation Standard:

The surveillance alerts generated by our internal and FIN KORP Software system based on the DP and Trading operations, Risk profile, Client Due Diligence and UCC / KYC details of the Clients, the and those provided by the Exchanges, Depositories and other regulators shall be conducted under the overall supervision of compliance officer in coordination with the staff, senior management along with the Principal Officer and the designated Director .

The Surveillance systems and internal controls are built in a manner that are commensurate with the complexity of the transactions done by our clients and our business activities The surveillance alerts generated by our FIN KORP Software system based on the Clients Trading, DP, Demat holdings, funds flow activities, Risk profile, Income Range, Occupation, common demographic details, frequent changes in KYC details, frequent off market Trades, Irrational Pledge transactions, dealing in illiquid shares or derivatives, dealing in concentrated trades, dealing in high values not commensurate with income or occupation, dealing as a group with concentration in specific scrip, unable to establish proper reason or logic on the transactions executed by the client, and any other irrational activities, and UCC / KYC details of the Clients as per our surveillance mechanism shall be continuously monitored on ongoing process by our trained staff under the supervision of Surveillance team, the Principal Officer and the Designated Director.

All our staff and associates are adequately trained to monitor the surveillance of client behavior through analyzing the pattern of trading and DP activities done by our clients, detection of any unusual activity being done by such clients and escalate the

suspicious transaction as laid down under the policy to the Surveillance team, the Principal Officer. Appropriate measures will be initiated after verifying the genuineness of the alerts, as per the policies and CDD measures to prevent any kind of fraudulent activity in the market in terms of the regulatory requirements prescribed by SEBI and Market Infrastructure Institutions (MIIs). Any Suspicious transaction shall be reported to the Exchanges,

Depositories, FIU IND and any other regulators as per the PMLA and other policies laid down by the Company at a period less than 48 hours from the detection of Suspicious transaction without tipping off.

Client Screening and Due Diligence:

We shall strictly adhere to the KYC guidelines as prescribed by SEBI, Exchanges, KRA and CKYC. CDD shall be carried on an ongoing basis.

We shall not allow any client to trade unless they have complied with the KYC Guidelines and the KYC is approved by the KRA. All the latest KYC details and information shall be updated to the KRA. Depositories and Exchanges.

We shall be continuously following the SEBI Master circular on AML on client screening and due diligence

Responsibility:

- "the **Compliance Officer** shall be responsible for the implementation and supervision of this Policy.
- The **Risk Management Officer**, Settlement Officer & PMLA Officer shall assist and report to the Compliance Officer on a daily basis in respect of the alerts generated for the surveillance mechanism.
- The Compliance Officer shall take all necessary steps to analyze, monitor, document and report the findings to the Board Members as well as the relevant Stock Exchanges and/ or regulatory bodies, in a time bound mariner, as detailed hereunder and/ or as mandated by the Stock Exchanges and/ or regulatory bodies.
- The Compliance Officer shall exercise their independent judgment and take adequate precautions to ensure implementation of an effective surveillance mechanism, based on the day-to-day activities of the clients, general mark t *information and the facts and circumstances.
- The Internal Auditor of the Company, shall review the Policy, its implementation, documentation, effectiveness and review the alerts generated during the period of audit and shall record the observations with respect to the same in their Internal Audit Reports.
- The Board of Directors shall peruse review and provide necessary guidance with regard to the "Surveillance Policy", periodically, for strengthening the processes.

Type of Alerts to be generated and/or reviewed:

S.No	INDICATIVE THEMES (Trading Related)
1.	Client / group of clients accounting for a significant percentage of the total trading activity in a scrip / contract as compared to the market.
2.	Client / group of clients with new account or clients dealing after a significant time gap, as accounting for significant value / percentage of total trading activity in a scrip / contract as compared to the market.
3.	Client / group of clients dealing frequently in small quantities/minimum market lot in a scrip / contract.
4.	Disproportionate trading activity vs reported income / Net worth.
5.	Frequent changes in KYC submitted by clients.
6.	Based on an announcement by a listed company, Client / group of clients, having possible direct / indirect connection with a listed company, who have undertaken any suspicious trading activity prior to price sensitive announcement by said listed company.
7.	Client / group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list'
8.	Consistency in profit / loss at client / group of clients' levels, rationale for such trading activities.
9.	Significant trading activity in shares by client who has pledged the shares of same scrip.
10.	Trading activity of a client or a group of clients in a scrip, the orders are being placed by respective clients or their authorized representatives and monitoring client's address as per KYC vis-à-vis the dealing office address
11.	Trading activities of accounts of relatives of entity to identify any sort of synchronized / coordinated trading.
12.	Surveillance / monitoring of IP addresses of clients (including identification of multiple client codes trading from the same location)
13.	Client/Group of Client (s), dealing in common Shares/Commodities.
14.	Pump and Dump
15.	Order book spoofing i.e. large orders away from market
16.	Front Running
17.	Internal Match Trade
18.	Debarred PAN client Traded

Factors to be considered for generating alerts:

ALERT	DESCRIPTION OF THE ALERT	CRITERIA FOR GENERATING ALERTS
1.	Client / related group of clients has large share of traded volume in a particular security in cash segment	Volume as 30 % of daily exchange volume
2.	Client / related group of clients has a large share of traded volume in contracts of a particular underlying.	Volume as 20% of daily exchange volume.
3.	Client / related group of clients dealing in illiquid shares near the price bands in small quantities.	5 continuous trading Days.
4.	Margin obligations disproportionate to declared income / Net worth (peak of the month)	If more than max 2 times the Net Worth or 8 times the peak of income range.
5.	Net funds pay-in/ pay-out during a period (one month) disproportionate to declared income/ Net worth	If more than max 2 times the Net Worth or 8 times the peak of income range.
6.	Frequent changes in any element of KYC (for mule accounts)	6 times of such changes of same element in an year.
7.	Client / related group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list'(SMS)	Value Exceeding Rs. One Crore
8.	Clients making net profit/ losses over a period which is a significant amount as compared to their income/ Net Worth in cash segment beyond a particular threshold	If more than max 1 time their Net Worth or 2 times the peak of income range.
9.	Order placed by multiple unrelated clients from the same IP/ device in case of internet-based trading clients.	If more than 6 clients.
10.	Repeated failure to deliver securities for pay-in obligations leading to auction/ close out in illiquid items (for reasons other than shortage of payout received in previous settlement)	If more than 4 times in a month
11.	Circular trading/Reversal pattern at same Trading Member above a threshold over a period of 1 month	Where profit / loss is more than Rs. 20 Lakhs.
12.	Front Running by Dealers/Clients to large trades of the Trading Member	Repeated trades by dealer in same security and before order of more than INR 0.50 Crores done in the firm
13.	Substantial proportion of the market open interest in a particular commodity / contract	If more than 5%.

The Principal Officer (PO) / Designated Director (DD) are empowered to decide and alter the thresholds along with documented rationale as per the business needs.

The above review shall also include the alerts generated by the Exchanges and Depositories:

All the Internal / Exchange/Depository alerts shall be reviewed periodically by the Principal Officer at least every 30 days till such time the alert is open.

Trading Terminals:

Trading terminals are allotted to Branches/HO/Authorised Persons only after updating the details to the Exchanges. We shall continuously monitoring the Login details of the trading terminals to ensure that the terminals are operated by the respective NISM certified Dealers only at the location notified to the Exchanges only and that none of the clients have direct operational access in any manner. The audit team through its intelligence reports by way of monitoring the attendance register/CC TV and surprise visits/random inspections shall ensure the compliance of the same.

To detect and prevent mule/ suspicious Activities as per our Standard Operating Procedure (SOP), we shall ensure that Authority to operate trading account is allowed to only family members in case of Individual Accounts and Employees /Group Company Employees/Apex body members - Directors, Partners, Trustees, etc. and Promoter/ Promoter group only, In case of other than Individuals. All such authorizations are allowed on being satisfied and declarations to that effect obtained.

All our Employees/Associated/ Authorised Persons are trained to identifies any fraud, market abuse, suspicious activity and the same shall be immediately to the senior management. We shall be communicating the responsibly of such an obligation to all our Employees /Associated/ Authorised Persons through webinars/ training programs/ written/ mail communication at a period not more than one year.

Guidance on factors to be assessed while reviewing the alerts:

Creation of misleading appearance of trading:-Trading of a security that occurs at specified prices, volumes and time in a manner agreed upon by the market participants in an attempt to match each other's trades. It may involve a group of clients and/or 'Authorised Persons' acting in concert. Such trading behavior has the effect of creating a false or misleading appearance of active trading in the security.

- In this regard, we identify potential connections and relationships among clients based on KYC data. We scrutinize the frequency and volume of matched trades that indicate pre-arranged, wash, or circular trading. Furthermore, we monitor factors such as market impact, trades involving disproportionate volumes, the proximity of order entry times, and the limits established by brokers based on the size of their business operations.

Price manipulation:-Trades that have the effect of artificially raising or lowering the market price of a security may create a false market. Greater scrutiny shall be emphasized on shares/commodities which cause significant price movements.

- Our compliance team monitors various activities described below, such as unusual price fluctuations; trades executed during sensitive periods—such as month-end or quarter-end, or prior to an announcement; trades that trigger significant price volatility; and limits established in accordance with our policy.

Front Running:-Trades undertaken while being privy to a big client order

- In this regard, the compliance team monitors to ensure that there is no time lag between front-running orders and orders placed by large clients. Furthermore, the team monitors factors such as the pricing of front-running orders—specifically whether they are identical to or better than other orders—while also keeping a close watch on their frequency, recurring patterns, and any unusual profit patterns.

Insider Trading:-Trading in securities that are listed or proposed to be listed on a stock exchange when in possession of unpublished price sensitive information.

- In this regard, the Compliance Team monitors the following aspects: whether any clients are trading at the time of a material announcement; whether profit patterns are unusual; whether trading patterns are unusual; whether clients are associated with listed companies; whether clients have realized substantial profits during the time of a material announcement; and so forth.

Un Authorised Trading: Trades executed in client's account taking instructions on orders from a third party ('Authorised Person'/Member/any person) with or without the client's prior authorization.

- In this regard, the Compliance Team monitors 'Authorized Persons' whose accounts exhibit unusual or highly irregular activity—for instance, cases where a single mobile number or email address is linked to multiple distinct client accounts, or where an excessive number of trading accounts have been opened or managed under the name of a single individual, among other such instances.

Order Spoofing: Places large orders to create the impression of Huge sale or Buy and cancels them on taking advantage of the situation on the Traded/Placed Orders already executed by him and covering the same

- In this regard, the Compliance Team monitors orders that are repeatedly placed and cancelled, or orders placed significantly above or below market rates.

Conflict of Interest:

In order to maintain utmost confidentiality and avoid tipping of information on all the Alerts generated and Reported on the surveillance activates, As per the policy we have identified the surveillance department as critical and no other person other than the authorized surveillance team shall have physical access to all the records, information and activities. Chinese Wall policies and procedures are adopted to prevent

unauthorized exchange of information between critical and non-critical departments.

Whistleblower Policy:

We have established a Whistleblower Policy to foster trust within the securities market. Its objective is to prevent and detect fraud or market abuse. Furthermore, it aims to facilitate the raising of concerns regarding suspected fraudulent, unfair, or unethical activities; violations of regulatory or legal requirements; or governance-related weaknesses.

We have constituted a Whistleblower Committee under the supervision of our Principal Officer, Mr. Manoj Agarwal, and our Nominated Director, Mr. Mahesh Mittal. These two individuals shall serve as the Whistleblower Complaint Redressal Heads and shall be responsible for reviewing complaints, while operating under the guidance and directives of the Whistleblower Committee.
In accordance with this Policy, any individual may register their concerns or complaints via a dedicated email ID—compliance@fairinvest.co.in—or by post addressed to 'Compliance/Redressal Head, Fair Intermediate Investment Pvt. Ltd., 2nd Floor, Shukla Palace, Sapru Marg, Lucknow, Uttar Pradesh 226 001'.

We have established procedures designed to ensure the complete protection of the whistleblower's identity—specifically, their confidentiality and anonymity. We guarantee that they will be treated fairly and will not face any form of adverse employment-related action, such as demotion, suspension, intimidation, harassment, or discrimination.

The Whistleblower Committee shall convene a meeting within 15 working days of receiving a complaint under these regulations and shall take appropriate action in accordance with the Policy.

The Whistleblower Complaint Redressal Heads shall conduct an initial review of the complaint and submit a report on their findings to the Whistleblower Committee. Based on the veracity of the complaint, the Committee may order a detailed investigation. If the complaint is directed against the Board of Directors, Key Managerial Personnel, the CEO, Managing Directors, or Promoters, it shall be referred to the Audit Committee; conversely, if the complaint is directed against an employee, it shall be referred to the Compliance Officer. The Compliance Officer shall ensure that this Policy is implemented in strict accordance with SEBI guidelines.

Any false complaint made with malicious intent shall be viewed seriously, and disciplinary action shall be taken against the offender as per the decision of the Management.

To ensure the effectiveness of this Whistleblower Policy—or whenever there are any amendments or changes to the regulations—it shall be subject to annual review and approval by the Board.

Policy Procedures for Disposition of Alerts:

- **Downloading of Transaction Alerts:** The Transaction Alerts provided by the Stock Exchanges and internally generated by the Back-Office Software shall be downloaded by "The Risk Management Team" on a regular basis and the same shall be forwarded to the Designated Directors, Compliance Officer and the KYC Officer.
- **Client(s) Information:** The "KYC- Officer" shall carry out the necessary Due Diligence of the client(s), whose name appears on the Transaction Alerts. The said officer shall ensure that the KYC parameters are updated on a periodic basis as prescribed by Securities & Exchange Board of India (SEBI) and latest information of the client is updated in UCC database of the respective Exchanges. Based on the Client Information, the said officer shall establish Groups/ Association amongst clients to identify multiple accounts/ common account/ group of clients
- **Documentation:** The Risk Management Team in order to analyze the trading activity of the Client(s)/ Group of Client(s) or scrips identified based on the Transaction Alerts, shall do the following:
  - Seek explanation from such identified Client(s)/ Group of Client(s) for entering into such transactions.
  - Seek documentary evidence such as Bank Statement/ Demat Transaction Statement or any other documents to satisfy it-self.
  - In case of Funds, Bank Statements of the Client(s)/Group of Client(s) from which Funds pay-in have been met, to be sought.
  - In case of Securities, Demat Account Statements of the Client(s)/Group of Client(s) from which Securities pay-in have been met, to be sought.
  - The period of such statements mentioned in point (c) & (d) may be at least
  - +/- 15 days from the date of transactions to verify whether the funds/ securities for the settlement of such trades actually belongs to the client to whom the trades were transacted.
- **Analysis:** Upon receipt of the above-mentioned documents, the Compliance Officer and the Risk Management Team shall analyze the documents sought from the Client as well as the KYC & KRA of the Client and shall record the observations for such identified Transactions or Client(s)/ Group of Client(s). In case adverse observations are recorded, the Compliance Officer shall report all such instances to the Exchange within 45 days of the alert generation.

Steps to be taken for analysis of each alert by Compliance Team:

Alert Generation System: Commensurate with our business transactions and behavior of our clients to have adequate surveillance systems in place, to customize our surveillance systems and internal controls the alerts are generated by our FIN KORP software internally and by the Depositories and the Exchanges are monitored by our Surveillance team.

Quality of Dealing:

- Identify scrips in BE, T and TS having 50 % of Exchange volume.
- Segregate the scrip volume based on the security category (e.g., EQ and BE in case of NSE and A, B, T, in case of BSE).
- Identify the clients and check the bonafide of transactions.

High Value Deals:

- Review the deals above Rs.25 Lacs in single scrip.
- in case of buy deals, check whether sufficient margin is available.
- In case of sale deal, check whether the shares are available.
- Identify scrips where deals are persistently contributing higher volumes.
- Identify clients, who have taken high value positions, review their ledger accounts in order to verify whether there is sudden increase in.

1. **Significant increase in client activity: Client(s)/Group of Client(s) who have been dealing in small quantities/value suddenly significantly increase their activity. In such cases the following shall be examined:**
   - Transaction Turnover more than Rs.10.00 Lacs.
   - Delivery Turnover more than Rs.2.00 Lacs
   - Deal size more than 2 times of the average deal size
     - Whether such volume is justified given the background of the client and his past trading activity.
     - Cumulative amount of funds that was brought in by the Client(s)/ Group of Client(s) for the purchases made during the period.
     - Whether such inflow of funds is in line with the financial status of the client.
     - Whether the transactions of such Client(s)/ Group of Client(s) are contributing to concentration or imparting the price.

2. **Sudden trading activity in dormant accounts:** This refers to such cases where the client has not traded more than 3 months and suddenly starts/resumes trading in stocks or low market capitalized scrips or enters into transaction which is not in line with his financial strength. In such cases following shall be reviewed and examined:

   - Trade Gap Analysis for more than 90 days.
   - Reasons for Trading in such scrips/contracts.
   - Whether the client is only placing the order or is it some third party.
   - Whether there is any concerted attempt by a Client(s)/Group of Client(s) to impact the prices of such scrips/ contracts through use of such dormant accounts.

3. **Clients/Group of Client(s), dealing in common scrips: Such dealing is contributing significantly to the volume of the scrip at broker level and at the Stock Exchange level. The following shall be reviewed and examined:**

   a. Reasons for trading in such scrips.
   b. Whether there is any concerted attempt by a client(s)/Group of Client(s) to impact the prices of such scrips.
   c. Whether there is any concerted attempt by a client (s)/Group of Client(s) to indulge in movement of profit/loss from one client to another.
   d. In case a client/ group of clients contributed more than 40% volume at Exchange level, repeatedly in the same scrip in last fifteen-day, client(s) is / are accumulating the scrip.
   e. Check if client(s) is/ are transferring the same to third party Demat A ccounts through off- market transactions.

4. **Client(s)/Group of Client(s) concentrated in a few illiquid scrips: The following shall be reviewed and examined:**

   a. Typically, the Risk Management 'Team shall block trading in scrips which are listed as Illiquid Scrips by the Stock Exchanges through its circulars.
   b. Any trading in such scrips are done on specific request by client, and the same is allowed by the Compliance Officer only upon scrutiny of the beneficial ownership of the selling, pre-pay-in of funds by the buying client and trades are executed at the last traded price.
   c. Activity concentrated in illiquid scrips.
   d. Sudden activity in illiquid securities
   e. Reasons for trading in such scrips.

   - Whether there is any concerted attempt by a Client(s)/ Group of Client(s) to impact the prices of such scrips.
   - Whether there is any concerted attempt by a Client(s)/ Group of Client(s) to indulge in movement of profit/loss from one client to another.
   - Percentage of Client(s)/ Group of Client(s) activity to total market in the scrip/contract is high.
   - Identify clients who have traded in these scrips more than 25% of Exchange volume.

5. **Client(s)/Group of Client(s) dealing in scrip in minimum lot size¡/Concentration in scrip: The following shall be reviewed and examined:**

   a. Reasons for such trading behavior.
   b. Whether the transactions of such Client(s)/Group of Client(s) are contributing to concentration or impacting the price.
   c. Whether such transactions indicate towards probability of illegal trading at the clients' end.

6. **Synchronized Trades/Cross Trades/Circular Trading:**

   a. Scrutinize Synchronized/Cross 'Trade Report generated by the system as well as the data published by the Stock Exchanges on their official website. Identify clients having cross or synchronized trades.
   b. Typically, any request for Block Deal is to be handled by the Risk Management Team directly under the guidance of Compliance Officer at the Head Office Level. Trades are to be executed only upon scrutinizing/ obtaining - proof of beneficial ownership of the selling client, proof of availability of funds by the buying client, pre-pay-in of shares of the selling client, pre-pay-in of funds by the buying client. Upon complying the same, trades are to be executed at the last traded price to avoid any price distortion. The executions of such trades are to be reported to the Designated Director as a routine compliance.
   c. Continuous trading of client/group of clients in particular scrip over a period of time.
   d. Client/ group of clients contributing significant volume (broker and exchange level) in particular scrip - especially illiquid scrip.
   e. Possible matching of trades with a specific group of clients (like same trade number on both buy and sell side and/or immediate execution of order in illiquid scrip etc.).
   f. Possible reversal of trades with the same group of clients (like same trade number on both buy and sell side and/or immediate execution of order in illiquid scrip)

7. **Pump and Dump:**

   a. Risk Management Team to disallow trades for being executed at prices significantly away from the market and later on squaring off to earn significant profits.

8. **Wash Sales or Reversal of Trades:**

   a. Same Client(s)/ Group of Client(s) on both sides of the transaction. (i.e. same trade number on both the buy and sell side).

b. Reversal of transactions by same Client(s) or within same Group of Client(s) at significantly different trade prices within a short period of time says 3-4 days.
c. One client makes significant profit and other suffers a loss or apparent loss booking transactions in Illiquid contract/ securities including options.

9. Front Running:

a. Trading, by Client(s)/ Group of Client(s)/ employees, ahead of large buy/ sell transactions and subsequent square off have to be identified and such transactions have to be reviewed for determining front running.
b. There is a consistent pattern of Client(s)/ Group *of* Client(s)/employees trading ahead of large buy/ sell transactions.

10. Concentrated position in the Open Interest/high turnover concentration:

a. Client(s)/Group of Client(s) having significant position in the total open interest of a particular scrip.
b. Client(s)/Group of Client(s) not reducing/ closing their positions in spite of the scrip being in ban period.
c. Client(s)/Group of Client(s) activity accounts for a significant percentage of the total trading in the contract/ securities at the Trading member and exchange level.
d. Monitor the trading pattern of Client(s)/Group of Client(s) who have Open Interest positions/ concentration greater than equal to the thresholds prescribed.
e. Identify the scrips where there is sudden increase in volume or rate by comparing the Exchange volume.
f. Check whether Broker has contributed substantial volume (more than 25 %) in such scrips. Identify clients who have contributed more than 25 % of the volume at the Exchange. Check for intimation letter uploaded by the Stock Exchange for the purpose of Additional Margin.
g. Identify the clients who are trading frequently in the scrips (more than 3 times in last five days).

11. Order book spoofing i.e. large orders away from market

a. Consistent placement of large orders significantly away from the market with low trade to order trade ratio or canceling orders within seconds after placing them thereby creating a false impression of depth in a particular scrip/ contract
b. Repeated pattern of placement of large buy orders which are away from the market price and simultaneous placement of sell orders to benefit from price rise or vice-versa.

12. Impact of Trading Pattern on Price and Volume of the Scrip

a. Identify the days on which the client has taken concentrated positions in the scrip and Compare price and volume on the Exchange on said dates to ascertain whether:
    i. Increase in price or volume beyond 20%.
    ii. Client has taken positions at day's high or low rates.

13. Review of Client Receipts / Payments

a. Review of Receipts/ Payment details of the Client having unusual pattern of funds movement. Analyze the Receipts & Payments of the client on daily basis and on Q-to-Q basis. Daily Bank Reconciliation on a Maker- Checker basis to be conducted to scrutinize Dishonor of Cheques.

14. Relation of Client with the Management/ Promoters of the Company

a. Check whether the client is related to management or promoters of the company in whose scrip client is trading.
b. Also check whether the client is holding more than 1% of the shares of the company.

15. Review of KYC & Turnover Vis-à-vis Financial Income Submitted by Client

a. Review the KYC and supporting documents submitted by the client.
b. Validate volume done by the client with his financial net worth and margin provided.
c. Identify the clients whose turnover is disproportionate with the Annual Income provided in KYC.
d. Review the Risk categorization of the client and categorize the client based on the validation done.
e. Scrutinize the Transactions of the clients and follow up with the concerned branches for collection of the latest financials. Seek details from Branch on the occupation, social and financial status of client. If Branch feedback on client is not satisfactory, refer the case to the Principal Officer.

Graded Surveillance Measures (GSM):

In continuation with the various measures implemented above to enhance market integrity and safeguard interest of investors, the Compliance Officer and Risk Management Team shall also implement the Graded Surveillance Measures (GSM) on securities that witness an abnormal price rise that is not commensurate with financial health and fundamentals of the company.

At present, there are 6 stages defined under GSM framework viz. from Stage I to Stage VI. Surveillance action has been defined for each stage. Once the security goes into a particular stage, it shall attract the corresponding surveillance action. Stage wise Surveillance actions are listed below —

Stage	Surveillance Actions
01.	Transfer to Trade for Trade with price band of 5% or lower as applicable.
02.	Trade for Trade with price band of 5% or lower as applicable and Additional Surveillance Deposit (ASD) of 100% of trade value to be collected from Buyer.
03.	Trading permitted once a week (Every Monday) and ASD of 100% of trade value to be collected from Buyer.
04.	Trading permitted once a week (Every Monday) with ASD of 200% of trade value to be collected from Buyer.
05.	Trading permitted once a month (First Monday of the month) with ASD of 200% of trade value to be collected from Buyer.
06.	Trading permitted once a month (First Monday of the month) with no upward movement in price of the security with ASD of 200% of trade value to be collected from Buyer.

The Risk Management Team has to be extra cautious and diligent while dealing in such securities as they have been placed under higher level of surveillance. A file containing stage wise GSM details is available on the website of NSE and BSE at the following link:

https://www.nseindia.com/invest/content/equities_surv_actions.htm

https://www.bseindia.com/markets/equity/EQReports/graded_surveil_measure.aspx

GSM framework shall work in addition to existing actions undertaken by the Exchange on the company's securities.

Additional Surveillance Measure (ASM)

The Compliance Officer and Risk Management Team shall also implement Additional Surveillance Measure along with the aforesaid measures on securities with surveillance concerns based on objective parameters viz Price variation, Volatility etc.

The shortlisting of securities for placing in ASM is based on objective criteria covering the following parameters:

- High Low Variation
- Client Concentration
- No. of Price Band Hits
- Close to Close Price Variation
- PE ratio

The surveillance actions applicable for the shortlisted securities are as under:

- Securities shall be placed in Price Band of 5% or as directed by the Stock Exchange(s) from time to time
- Margins shall be levied at the rate of 100%.

ASM framework shall be in conjunction with all other prevailing surveillance measures being imposed by the Exchanges from time to time.

Unsolicited Messages (SMS Stock)- FIIPL)

Clients are advised to remain cautious on the unsolicited emails and SMS advising investor to buy, sell or hold securities and trade only on the basis of informed decision.

Investors are also requested to share their knowledge or evidence of systemic wrongdoing, potential frauds or unethical behavior through the anonymous portal facility provided on Exchange website and mail at the following addresses:

- **invg@nse.co.in**
- **investigation@bseindia.com**

Clients to exercise caution towards unsolicited emails and SMS and also request their clients to buy, sell or hold securities and trade only on the basis of informed decision. t?1ients are further requested not to blindly follow these unfounded rumors, tips etc. and invest after conducting appropriate analysis of respective companies.

In view of above & as a part of surveillance measure to protect investor's interest and maintain market integrity, Exchange has advised members to exercise greater caution with respect to tips / rumors circulated via various mediums such as analyst websites, social networks, SMS, What's App, Blogs etc. while dealing in the securities listed on the Exchange on behalf of their clients.
The Securities identified by Exchange(s) in which unsolicited SMS are circulated shall be kept suspended and barred from further buying & selling by us and shall be monitored on regular basis.

The Clients shall remain cautious on the unsolicited emails and SMS advising to buy, sell or hold securities and trade only on the basis of informed decision.

Broker may in exceptional circumstances, where the Client has dealt in "SMS Stocks, shall withhold the pay-out of funds and/ or securities of the Client and/or suspend the Demat Accounts for Debits, without assigning any reasons, to adjust the Traded Value of Trades in such SMS Stocks with retrospective effect and transfer the same to the Designated Bank Account earmarked for this purpose as mandated by Stock Exchange(s)/SEBI from time- to-time and retain the same till directed by the Stock Exchange(s)/SEBI for such release.

Surveillance in respect of Depository Participant

Generation of suitable surveillance alerts which may be guided by indicative themes given in point no. 2 below (the list is inclusive and not exhaustive).

Review and disposal of transactional alerts provided by CDSL. (Transactional alerts provided by CDSL are based on certain thresholds.

Disposal of alerts within 30 days from the date of alerts generated at Participants end and alerts provided by CDSL. Reporting to CDSL and other authorities as applicable in case of any abnormal activity. Documentation of reasons for delay, if any, in disposal of alerts.

Framework of appropriate actions that can be taken by the Participant as per obligations under Prevention of Money Laundering Act (PMLA).

Purpose and Scope

Purpose: To define a workflow for creating, investigating, and resolving surveillance alerts to ensure market integrity.

Scope: Applies to all transactional and demographic alerts, whether generated internally or received from depositories (CDSLs) and exchanges.

Indicative themes based on which alert should be generated and maintained and reported as per the requirement:

Sr. No.	Indicative themes:
01.	Alert for multiple demat accounts opened with same demographic details: Alert for accounts opened with same PAN /mobile number / email id/ bank account no. / address considering the existing demat accounts held with the DP.
02.	Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
03.	Frequent changes in details of demat account such as, address, email id,mobile number, Authorized Signatory, POA holder etc.
04.	Frequent Off-Market transfers by a client in a specified period
05.	Off-market transfers not commensurate with the income/Net worth of the client.
06.	Pledge transactions not commensurate with the income/Net worth of the client.
07.	Off-market transfers (High Value) immediately after modification of details in demat account
08.	Review of reasons of off-market transfers provided by client for off-markettransfers vis- à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts/Donation to unrelated parties, frequent transfers with reason code off-market sales
09.	Alert for newly opened accounts wherein sudden Increase in transactions activities in short span of time and suddenly holding in demat account becomes zero or account becomes dormant after some time.
10.	Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.
11.	Multiple demat accounts of different entities being opened with a common bank account.
12.	Accounts were opened by obtaining multiple PANs by single entity
13.	High Volume/ Value Dematerialization Alerts
14.	Transaction in Dormant Account
15.	High Value Credit/ High Quantum Credit / High value Gift or Donation Credit
16.	High Value Debit / High Quantum Debit / High value Gift or Donation Debit
17.	High Volume/ Value Preferential Allotment
18.	Significant Holding in Listed Scrip
19.	High Volume/ Value Off-market transactions in scrip appearing in GSM OR ASM list published by exchanges
20.	Others (Transfer of Suspended shares, any other concerns

The Principal Officer (PO) / Designated Director (DD) are empowered to decide and alter the thresholds along with documented rationale as per the business needs.

The above review shall also include the alerts generated by the Exchanges and Depositories:

All the Internal / Exchange/Depository alerts shall be reviewed periodically by the Principal Officer at least every 30 days till such time the alert is open.

Alert Genration Parameters:

Alerts are triggered based on predefined as mentiond below:

S.NO.	Parameters of Alerts to be generated	Alerts to be reported	Base for reporting of Alerts
01.	Alert for multiple demat accounts opened with same demographic details:	Demographic details is in more than 2 demat accounts	Demographic details wise
02.	Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.	All instances	Client ID wise
03.	Frequent changes in details of demat account	Changes is executed more than 2 times whithin a month	Client ID wise
04.	Frequent Off-Market transfers by a client in a specified period	Off market transfers executed mote than 5 times	Client ID wise
05.	Off-market transfers not commensurate with the income/Net worth of the client.	All instances- Limit given up to 10 times	Client ID wise
06.	Pledge transactions not commensurate with the income/Net worth of the client.	All instances- Limit given up to 10 times	Client ID wise
07.	Off-market transfers (High Value) immediately after modification of details in demat account	All instances	Client ID wise
08.	Review of reasons of off-market transfers provided by client for off-markettransfers vis-à-vis profile of the client	All instances	Client ID wise
09.	Alert for newly opened accounts wherein sudden Increase in transactions activities in short span of time	All instances	Client ID wise

Roles and Responsibilities

Role	Responsibility
Maker (Analyst)	Downloads alerts, conducts initial due diligence, collects client rationale, and proposes closure or escalation.
Checker (Manager)	Reviews the Maker's findings, validates supporting documents, and approves the disposal.
Compliance Officer	Oversees the entire process, reports "Adverse Observations" to regulators, and reviews the SOP annually.
Principal Officer	Final authority for filing Suspicious Transaction Reports (STR) with FIU-India.
IT support	Maintains and updates the monitoring system
Senior management	Oversees the effectiveness of the monitoring process.

Alert Generation Parameters

Alerts are generated based on predefined "themes." Key indicators include:

- **Demographic Alerts:** Multiple accounts with the same PAN, mobile number, or email; frequent changes in KYC details (address, bank, etc.).
- **Transactional Alerts:** High-value off-market transfers; transactions not commensurate with the client's declared income/net worth.
- **Behavioural Alerts:** A new account showing a sudden surge in volume followed by immediate dormancy; frequent "Gift" reason codes for transfers to unrelated parties.
- **Market Alerts:** Concentrated trading in illiquid or ASM/GSM (Additional/Graded Surveillance Measure) stocks.

Operational Workflow

- **Step 1: Alert generates & Triage**
- **Frequency:** Alerts from the depository are typically processed on a weekly/monthly basis. Internal alerts are reviewed daily (T+1).
- **Alert Generation:** The monitoring system automatically creates alerts based on predefined rules and thresholds set by regulatory bodies and internal risk management teams
- **Step 2: Initial Analysis (Maker)**
- The Maker reviews the client's past trading/holding patterns. It is determined whether the client's transaction values match the income range and activity recorded in the account.

Step 3: Reason for request

If any activity appears suspicious, Maker contacts the client via registered email/phone, asking for the reason and supporting documents (e.g., bank statement, demat statement, income proof, KYC proof) if required. This is also updated in the database of all portals used by the company.

Detailed Analysis: Additional investigations are applied to high-risk alerts.

- Compliance may investigate further or request additional information
- Periodic reports are generated for review by senior management.
- Regular updates and improvements are made to alert parameters based on trends and regulatory changes.
- Periodic compliance audits and self-assessments.
- Emergency measures can be implemented in case of system failures or major security threats.

Exception Handling: Any deviations from the SOP should be documented and approved by senior management.

Verification & Disposition

- **False Positive:** If the explanation is valid and documented, the Maker marks it for closure with "Satisfactory Rationale."
- **Genuine Alert:** If the client fails to provide a rationale or the activity indicates manipulation, the Maker marks it as "Adverse."

Step 4: Maker-Checker Review

The checker reviews the case. If satisfied, they authorize closure. If more information is needed, the alert is returned to the maker for revision.

Timelines & Reporting

Regulatory compliance requires strict adherence to the following timelines:

Activity	Deadline
Review & Disposal	Within **30 days** of alert generation.
Adverse Observations	Report to Depository within **7 days** of identification.
STR Filing	As per PMLA guidelines (usually within 7 days of concluding suspicion).
MIS to Board	**Quarterly** (summary of pending, closed, and reported alerts).

Training and Awareness

Regular training sessions for staff involved in surveillance activities.
Awareness programs to keep staff informed about emerging risks and compliance updates

Compliance and Regulatory Requirements

Adherence to guidelines issued by regulatory bodies such as SEBI, RBI, and relevant exchanges

Time Frame for Disposition of Alerts:

The above procedure should be completed within 15 calendar days from the last trading day of the month. In case the matter prolongs beyond 15 days the same should be reported to the Board of Directors, by the Compliance Officer, citing reasons for such delay. The Compliance Officer may seek extension of the time period from the Exchange, whenever required, under intimation to the Board of Directors.

Management Information System (MIS):

A Monthly MIS Report shall be put up by the Compliance Officer to the Board of Directors on the number of alerts pending at the beginning of the month, generated during the month, disposed off during the month and pending at the end of the month

Internal Auditor shall verify and submit separate report with regard to “Surveillance Policy” on a monthly basis and the actions taken in respect o1 the Compliances made and pending actions, if any.

Record Maintenance & Reporting

The Compliance Officer shall be responsible for all surveillance activities carried out by the Company and for the record maintenance of such activities.

The Compliance Officer shall be assisted by the Risk Management Team and the KYC & KRA Officer for the surveillance activities and shall have the discretion to take assistance/help from any professionals and/ or software for the better implementation of the surveillance activities, without diluting the accountability and responsibility of the Compliance Officer.

Each alert received from the exchange shall be backed by necessary supporting documentary evidence collected from clients, any other additional details as may be deemed fit may be captured and placed before the Board of Directors for review.

Trading Member shall report duly approved status of the alerts on a quarter basis to the Exchange/ Depository within 15 days from the end of the quarter in the prescribed format.

With Respect to Depository's Circular dated July 15th,2021 regarding "Surveillance Obligations for Depository Participants", We as Depository Participant with discussion with management has defined an internal criterion to identify the nature of alerts and process the necessary verification on the same. The alerts will be identified on the basis of below mentioned criteria as follows:-

Scrutiny and Disposal of the Transaction Alerts:

1. The DP Operations team shall be responsible for analysing the alerts raised basis the parameters defined above on a quarterly basis.

2. The following steps to be followed for analysing the transaction alerts raised internally by the DP Operations team:

a. System generated reports, wherever available to be downloaded within 5 days of the end of the each quarter.

b. Obtain transaction rationale and obtain such supporting documents as may be required from the client.

c. After analysing the documentary evidences, including the bank / demat statement, if any, the DP Operations team shall record their preliminary observations for such identified transactions or client(s) / group of client(s) and share the same with the Compliance Officer within 10 days from the date of generation of alerts.

d. In case the Compliance Officer concludes the adverse observation to the alert, he/she shall in form CDSL within 15 days from date of identification of adverse observation.

3. With respect to the transactional alerts provided by CDSL, the DP Operations team and the Compliance Officer shall ensure that all alerts are reviewed and status thereof (Verified & Closed/Verified & Reported to Depository) including action taken is reported to CDSL within 30 days as per the prescribed process by CDSL

4. The records of alerts generated, disposed of as closed and details of action taken wherever applicable shall be maintained either in physical or electronic format by the DP Operations team with such security measures as would make such records temper proof and the access is available on to designated officials under the supervision of the Compliance Officer.

Suspicious / Manipulative activity identification and reporting process

Suspicious / Manipulative activity identification and reporting process include gathering of client information, analyzing client activity, seeking documentary evidence required, monitoring the trading activities, record maintenance and reporting.

1. Client Information

- Implementing Anti Money Laundering Policy viz a viz KYC standard for new clients acceptance and implementing high standard of due diligence process.
- Periodic updating of client database and having system to do continues due diligence.
- Identification of Beneficial Ownership
- Identification of Multiple Accounts/common Accounts/group of clients
- Analyzing common emails, mobile numbers, address and other linkages
- Other publicly available information

2. Analysing Client Activity

Client' trading pattern or activity shall be analyzed based on Alert received/generated through exchange system. There are alerts which require only client confirmation or explanation or trading history analysis and there are other alerts which require documentary evidence viz. Bank Statement or Demat Statement for +/- 15 days as per Exchange requirements.

- ### Transaction Alerts falling under Sr. No. 1 & 2

It requires only trading history analysis, last 12 months trading turnover analysis, turnover v/s income range comparison and client confirmation on sudden activity in dormant account. Member shall also take reasonable steps to analyzed these type of alerts and shall be required to close the status of alerts or report the exchange in case of any adverse findings.

- ### In case of transactional alerts from Sr. No. 3 to 13,

Apart from analyzing trading history and income comparison, member shall take explanations regarding alerts received from the exchange and also ask for +/- 15 Days Bank Statement in case of Funds Movement and Demat Statement in case of movement of shares and Compliance Manager/Operation Manager shall verify whether the funds/securities for the settlement of such trades actually belongs to the client for whom the trades were transacted or not.

Members shall record observation for such transactional alerts and maintain records with regards to such analysis. In case, client failed to provide explanation or documentary evidences, such client shall be deactivated and shall be activated only after they satisfy all requirement of this policy.

Obligation of Quarterly reporting of status of the alerts generated by the Depository participants:

Status of Alerts generated by the Depository:

Name of Alert	Opening Balance of alerts at the beginning of the quarter (A)	No. of alerts generated during the quarter (B)	Total no. of alerts (C=A+B)	No. of alerts closed during the quarter (D)	Alerts pending at the end of the quarter (E = CD)	Ageing analysis of the alerts pending at the end of the Quarter (since alert generation date) (Segregation of E column)					Reason for pendency#
						< 1 month	1-2 months	2-3 months	3-6 months	> 6 months	

 # reason for pendency is required to be provided for outstanding alerts in each bucket of age.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For FAIR INTERMEDIATE INVESTMENT PRIVATE LIMITED

Policy created by: KULDEEP TRIVEDI

Policy reviewed by: Mansi Nagrath

Policy reviewed on: 05th Nov 2025

Policy approved by: Board of Directors

Policy approved on: 05th Nov 2025