

SWASTIKA INVESTMART LIMITED

SURVEILLANCE POLICY

Background:

The Stock Market Regulator/ Stock Exchanges / Depositories has directed its intermediaries/members / Depository Participant's to conduct surveillance in trading/Demat activity of their clients to ensure market integrity, regulatory compliance, enforcement of exchange/Depository rules, risk management, investor protection, and to gain insights for market surveillance and analysis.

Swastika Investmart Limited ("the Company") is registered with the Securities and Exchange Board of India ("SEBI") as a Stock Broker and Depository Participant and is engaged in securities market activities. The Company recognizes its responsibility to establish an effective surveillance mechanism to detect, monitor, investigate and report suspicious, unusual, manipulative or abnormal transactions and activities undertaken by clients.

This Policy has been framed in accordance with SEBI circulars, Exchange directions, Depository guidelines, Prevention of Money Laundering Act, 2002 ("PMLA"), Anti-Money Laundering ("AML") requirements, and surveillance obligations prescribed by CDSL, NSDL, NSE, BSE and other regulatory authorities.

The objective of this Policy is to strengthen the surveillance framework of the Company and ensure timely identification and reporting of suspicious activities in trading and depository accounts

Thus, exchange/depositories have advised its members/Depository Participant's to frame a surveillance policy covering following:

1. Obligation of Trading Member/Depository Participant to frame Surveillance Policy
2. Obligation of Trading Member/Depository Participant to generate additional surveillance alerts
3. Obligation of trading member /Depository Participant with respect to client due diligence
4. Observation of Trading member/Depository Participant with respect to processing alerts
5. Time frame for disposition of alerts and if there is any delay in disposition, reason for the same should be documented.
6. Identification of any Suspicious/Manipulative activity and reporting the same.
7. Quarterly reporting of alerts
8. Record Maintenance.

SCOPE:

This Policy shall apply to:

1. Stock Broking operations;
2. Depository Participant operations;
3. Equity, F&O, Currency and Commodity segments, where applicable;
4. Branch offices and Authorised Persons;
5. Employees, dealers and relationship managers;
6. Back-office and operations teams;
7. Compliance and surveillance teams.

The Policy shall cover:

1. Trading transactions;
2. Demat account transactions;
3. Off-market transfers;
4. Pledge and unpledge transactions;
5. Client onboarding activities;
6. Fund movement patterns;
7. Suspicious transaction monitoring

Obligation of Trading Member/Depository Participant to frame Surveillance Policy

It is mandatory under the exchanges/Depositories regulatory directives to have in place appropriate Surveillance Policies and Systems to detect, monitor and analyze transactions.

A. Transactional alerts as generated from the exchange may include the following kind of alerts:

S.No.	Transactional Alerts	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 a few illiquid scrips	Cash
5	Client(s)/Group dealing in scrip in of Client(s) 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 (A wash sale is trading activity in which shares of a security are sold at a loss and a substantially identical security is purchased)	Cash & Derivatives
10	Reversal of Trades	Cash & Derivatives
11	Front running	Cash

12	Concentrated position in the Open Interest / High Turnover concentration	Derivatives
13	Order book spoofing i.e. large orders away from market	Cash

B. Transactional/Additional Alerts generated by Trading Member:

For effective monitoring of the Trading activity of Clients, the Company generate an additional alerts based on the below mentioned themes:

- a. 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.
- b. 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.
- c. Client / group of clients dealing frequently in small quantities / minimum market lot in a scrip / contract.
- d. Disproportionate trading activity v/s reported income / Net worth.
- e. Frequent changes in KYC submitted by clients.
- f. Based on an announcement by a listed company, identify 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.
- g. Client / group of clients having significant selling concentration, in the scrips, forming part of "For Information list" or "Current Watch list".
- h. Consistency in profit / loss at client / group of clients" levels, rationale for such trading activities.
- i. Significant trading activity in scrips by client who has pledged the shares of same scrip.
- j. In case of concerns of trading activity of a client / group of clients in a scrip, monitoring whether the orders are being placed by respective clients or their authorized representatives and monitoring client's address as per KYC vis-a-vis the dealing office address.
- k. Significant trading activity in scrips where client has pledged shares or has significant holding or has frequent off-market transactions.
- l. Surveillance / monitoring of IP addresses of clients (including identification of multiple client codes trading from the same location).

C. Transaction Alerts to be generated by Depository Participant :

For effective monitoring of the demat transactions of Clients, the DP's generates additional alerts based on the below mentioned themes:

Part A

- a. Alert for multiple demat accounts opened with same demographic details

- b. Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
- c. Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.
- d. Frequent Off-Market transfers by a client in a specified period
- e. Off-market transfers not commensurate with the income/Net-worth of the client.
- f. Pledge transactions not commensurate with the income/Net-worth of the client.
- g. Off-market transfers (High Value) immediately after modification of details in demat account
- h. Review of reasons of off-market transfers provided by client for off-market transfers 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
- i. 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.
- j. Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by clients.

Part B:

- a. Off-market transfer of securities from one demat account to many demat accounts without any economic rationale.
- b. Off-market receipt of securities from multiple demat accounts to one demat account without any economic rationale.
- c. Multiple demat accounts opened with noticeably short / incomplete address.
- d. Different demat accounts of same persons with different PANs.
- e. Demat accounts of a person used by another person for deceptive purposed.
- f. Multiple off-market transfers (value and volume based) with potentially incorrect offmarket reason code declared.
- g. Shifting of ownership of securities to avoid attachment of securities by government authorities or under IBC / NCLT.
- h. Fraudulent / unauthorised transfers in dormant demat accounts.

Due Diligence:

The Company will carry out the Due Diligence of its client(s) on an on-going basis. Further, the company shall ensure that key KYC parameters are updated on a periodically basis and latest information of the client is updated in Unique Client Code (UCC) database of the Exchange / Depository. Based on this information the Company shall establish groups / association amongst clients to identify multiple accounts / common account / group of clients.

Analysis:

In order to analyze the trading/Demat activity of the Client(s) / Group of Client(s) or scrips identified based on above alerts, the following steps are taken:

- a. Explanation/ Clarification/ Rationale is sought from such identified Client(s) / Group of Client(s) for entering into such transactions;
- b. Analyzing the past trading patterns of the client;
- c. Seeking documentary evidences such as bank statement/ Demat transaction statement or any other documents to commensurate it; and
- d. In case of funds, Bank statements of the Client(s) / Group of client(s) is sought, from whom funds pay-in have been met.
- e. In case of severe alerts, clients can be warned for stopping the activities and not to carry on further transactions with respect to the alerts.

After analyzing the documentary evidences, such as the bank / demat statement or any other relevant documents relevant to the said alert/ transaction, we shall record its observation for such identified transactions or Client(s) / Group of Clients(s). In case any adverse observations are recorded, we shall report all such instances to the exchange. In Order to sharpen the surveillance measures, it is emphasised that client due diligence and KYC are up to date which can minimize false positives, provide meaningful alerts and help identify related parties who are possibly (mis)using same details such as mobile number, email id, etc. Also, in terms of other information, the Depository Participants may attempt to obtain latest information about income ranges, bank details, address, nomination, etc.

Further, if there is a major disparity between financial details and trading volumes, client will be asked to furnish suitable explanation and based on the same further trading limits will be sanctioned. Additionally, an interim action inter-alia withholding the payout of client and suspend his trading account is taken against clients if they don't cooperate in furnishing required documents/ or if they don't respond.

These alerts are analyzed and appropriate measures are initiated wherever required, as per the policies and Client Due Diligence measures and may also report to Exchanges, Depositories, SEBI, any other Regulators or FIU IND as per the PMLA policies lay down by the company, as the case may be.

General Code for processing the alerts:**Part A**

- a. Depository Participants are required to maintain register (electronic/physical) for recording all alerts generated.
- b. While reviewing alerts, Depository Participant shall obtain transaction rationale, verify demat account statement and also obtain supporting documents as required from the client.
- c. After verifying the documentary evidence, Depository Participants shall record its observations for such identified transactions of its Client.
- d. With respect to the transactional alerts to be provided by Depository, Depository Participants shall ensure that all alerts are reviewed and status thereof (Verified & Closed/Verified & Reported to

Depository) including action taken is updated within 45 days, on the NSDL e-PASS portal.

e. With respect to the alerts generated at the Depository Participants end, DPs shall report instances with adverse observation, along with details of action taken, to NSDL within 7 days of the date of identification of adverse observation, on the NSDL e-PASS portal

Part B

f. Depository Participants are advised to refer alerts wise guidelines provided in the NSDL e-PASS portal while reviewing the alerts.

g. Depository Participants are required to adhere to the guidelines in letter and spirit in terms of resolving the alerts in a timely manner that is complete and does not result in rejection of the responses to the alert.

h. Any supporting document that is necessary to corroborate the responses by way of evidence i.e., copy of the account opening form, correspondence with the client, internal investigation reports etc. may also be provided.

Suspicious/Manipulative activity identification and reporting process:

After analysis of the transaction/alerts, documentary evidences and information available with us, we shall identify the suspicious/manipulative transactions of any of the client/group of clients, if any and shall report the same to the exchange within the prescribed time limit. Further we may stop/banned client for doing further trading at our end.

Frame for disposition of alerts:

In case adverse or suspicious observations/alerts are recorded, we shall report such instances to the exchanges/Depositories within 30 days of alert generation. In case there is delay, we shall seek extension of the time period from the Exchange/Depositories after giving proper reason for delay.

Quarterly reporting of alerts:

We are obligated to submit the quarterly reports of alerts generated within 15 days from end of quarter. The appropriate status of alerts generated at exchange/Depositories as well as alerts that are generated internally are required to be submitted on periodic basis in format as prescribed by exchange/Depositories.

Record maintenance:

We shall maintain and keep all such records and documentary evidences that has been analyzed/gathered by us either in soft copy or in hard copy for the time period as prescribed by the regulatory authority. We shall produce such records as and when asked by exchanges/Depositories or by any other regulatory authority.

Responsibility of The Compliance Officer/Designated Director:

1. The alert generation and monitoring is done under the supervision of the Compliance Officer.
2. A quarterly MIS report is prepared stating the alerts generated at the beginning of the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with the reason for the pendency and the action plan for the same.
3. The compliance officer to ensure timely generation and disposal of internal surveillance alerts.
4. The compliance officer of the Depository Participant shall ensure the quality of responses for closure of alerts using sampling method, in terms of completeness.
5. The compliance officer and internal auditor may provide their suggestions to improve the overall quality and effectiveness of surveillance operations, where necessary.

Internal Audit:

The internal auditor of the company reviews the Surveillance policy during the Internal audit being conducted for the company and will report the observations in the audit report.

Employee Awareness and Training:

Employees shall undergo periodic training on:

1. surveillance obligations;
2. suspicious transaction indicators;
3. regulatory requirements;
4. escalation procedures;
5. AML and fraud risk indicators;
6. reporting obligations.

The Company shall maintain records of training programs conducted.

Policy reviewed and authorized by:

The policy will be reviewed and amended whenever the new circular issued by regulators or any direction given by them or as and when considered necessary by the Board or if there is no amendments or circular issued by regulator then once in every year reviewed by the Board.

Review Date: 2nd May, 2026