



Nirman Share Brokers Pvt Ltd.

SURVEILLANCE POLICY

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, **Nirman Share Brokers Pvt Ltd.** would have in place adequate surveillance policies and system in order to monitor suspicious/manipulative transactions and curb such activities, if any.

Therefore, this Policy has been prepared in accordance with applicable Rules and Guidelines of SEBI and Exchanges/Depositories and is applicable to all our clients.

OBJECTIVE:

- To establish a surveillance mechanism and control in the operations/trading activity of the clients.
- Detection and reporting of suspicious trading activities in accordance with applicable laws/ laid down procedures.
- To comply with applicable laws and regulatory guidelines.
- Maintaining integrity of the market.
- Minimizing business risk through better profiling of clients and transactions.

SURVEILLANCE FRAMEWORK:

This policy covers the various surveillance alerts generated by us/ received from the exchange/depository for identifying suspicious trades, analysis of these alerts, methodology of reporting the alerts to the exchange/depository/FIU.

As it is mandatory under the exchange/Depository regulatory directives to have in place appropriate Surveillance Policies and Systems to detect, monitor and analyze transactions. For the above we have to co-relate the transaction data with their clients' information/data. Detect suspicious/manipulative transactions is an ongoing continuous process with analysis of trades and transactions and carrying out Client Due Diligence (CDD) on a continuous basis.

In-order to implement the exchange/depository directives, our surveillance desk downloads all the alert based on the trading activity of client provided by all the exchanges/depositories for detailed analysis.

In addition to the transactional alerts downloaded by Exchanges and DP, it is also required to generate appropriate surveillance alerts at our end, to enable us to effectively monitor the trading activity of our clients.

The details of all the various alerts have been enumerated below.

TYPES OF TRANSACTION ALERT BY EXCHANGE

Sr. No.	Transaction Alerts	Segment
1	Significantly increase in client activity	Cash
2	Sudden trading activity in dormant account	Cash
3	Clients/Group of Client(s), dealing in common Scrip	Cash
4	Client(s)/Group of Client(s) is concentrated in a few illiquid Scrip	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	Cash
9	Reversal of Trades	Cash & Derivatives
10	Front Running	Cash
11	Concentrated position in the Open Interest/ High Turnover concentration	Derivatives
12	Order book spoofing i.e. large orders away from market	Cash

FACTORS TO BE CONSIDERED FOR GENERATING ALERTS

The indicative themes on which NSBL may formulate their own alerts are as under:

Alert	Short description of the alert (based on alerts listed by exchanges in their circulars from time to time)	Factors to be considered for generating alerts
--------------	--	---

1	Client / related group of clients has large share of traded volume in a particular security in cash segment	1. Volume as % of daily exchange volume 2. Volume as % of the last 30 days exchange average volume (for QSBs only)
2	Client / related group of clients has a large share of traded volume in contracts of a particular underlying	1. Volume as % of daily exchange volume 2. Volume as % of the last 30 days exchange average volume (for QSBs only)
3	Client / related group of clients dealing in illiquid shares near the price bands in small quantities	Frequency of such trades
4	Margin obligations disproportionate to declared income / Networth (peak of the month)	If more than max (x times n/w or y times income)
5	Net funds pay-in/ pay-out during a period (one month) disproportionate to declared income/ Networth	If more than max (x times n/w or y times income)
6	Frequent changes in any element of KYC (for mule accounts)	Frequency of such changes of same element
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 of such sales
8	Clients making net profit/ losses over a period which is a significant amount as compared to their income/ Networth in cash segment beyond a particular threshold	If more than max (x times n/w or y times income)
9	Order placed by multiple unrelated clients from the same IP/ device in case of internet-based trading clients	If more than x 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 x times in a month
11	Multiple unrelated clients (more than X) being onboarded online from the same device (other than permitted e.g. whitelisted employees/ Authorised Persons (APs))	If more than x clients
12.	Circular trading/Reversal pattern at same Trading Member above a threshold over a period of 1 month	Where profit / loss is more than x

13.	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 x crores done in the firm
14.	Substantial proportion of the market open interest in a particular commodity / contract	If more than x%

We analyze the available factors and decide the thresholds as per our business size and risk involvement on transactions undertaken by client. We review our processes periodically and implement necessary procedures so as to comply with the regulatory requirements Thresholds to be determined byas per business size. The review report of thresholds shall be submitted to the apex body at least once a year.

TYPES OF TRANSACTION ALERT BY MEMBER

Sr. No.	Transaction Alerts
1.	Trading activity in a single day by one client or group of clients who have contributed more than 25% in a single scrip or a single derivative contract.
2.	A client or a group of clients who are either new client/ clients or who have reactivated their trading account after significant time gap and who have contributed more than 50% of the total trading volume of a single scrip or derivative contract in a single day.
3.	Client or a group of clients dealing frequently in small quantities in a scrip.
4.	Trading activity of a client found to be disproportionate considering a reported income range details or networth.
5.	A client who has submitted modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details etc. at least twice in a month.
6.	A client or a group of clients who have been found to have direct or indirect connection with a listed company and who have executed any transactions prior to any dissemination of any price sensitive information by such listed company.
7.	A client or group of clients having more than 20% volume of any scrip listed in for 'information list' or 'current watch list'.
8.	A client or group of clients which persistently earn or incur high amount of loss through their trading activities or clients who appear to have executed trades with the objective of transfer of profits or losses.
9.	A client who is holding more than 5% of paid up capital of a listed company and has pledged 100% of his/her/it's such holding for margin purpose and who has also significant trading volume in the same scrip which he/she/it holds.

10.	In case of a client or a group of clients who have been identified as per any of the above 9 criteria and whose orders are placed through a dealing office which is far from such client's address as per his/her/its KYC.
11.	A client having demat account with NSBL GROUP and who has holding in a scrip of more than 5% of paid up capital of a listed company which has received the same shares through off-market transfer.
12.	A client who has received shares of a listed company through multiple off-market transfer and has pledged such shares.
13.	Identification of IP addresses of clients to identify multiple client codes trading from same IP address.
14.	Clients who are connected with each other as per key KYC parameters of the clients as updated by respective client.
15.	Trading activities of accounts of relatives* of entity to identify any sort of synchronized / coordinated trading.

SURVEILLANCE FRAMEWORK FOR OPERATIONS AS DEPOSITORY PARTICIPANT:

CDSL is providing transactional alerts on biweekly basis based on threshold defined by CDSL to all the Depository Participants including NSBL GROUP through CDSL report download utility. As per applicable Communiqués, NSBL GROUP is reviewing these alerts and taking appropriate actions after carrying out due diligence viz. either disposing off alerts with appropriate reasons/findings recorded or filing Suspicious Transaction Report (STR) with FIU-India in accordance with the prescribed transactions and information for a minimum period up to eight years with provisions of PMLA (Maintenance of records) Rules, 2005.

*In addition to the same, **NSBL** GROUP has framed its Surveillance Policy to generate alerts as per guidance provided in CDSL Circular No. CDSL/OPS/DP/SYSTM/2021/309 dated 15.07.2021 based on following criteria:*

1.	<i>Multiple Demat accounts opened with same PAN/mobile number/ email ID/ bank account details/ address. While reviewing BO account details, the details of existing BO shall also be considered.</i>
2.	<i>Email/ letters sent to clients on their registered email ID/address which bounces/ returns undelivered.</i>
3.	<i>A BO who has submitted modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details, POA holder, Authorised Signatory etc. at least twice in a month.</i>
4.	<i>Frequent off-market transfer of securities more than twice in a month without genuine reasons.</i>
5.	<i>Off-market transactions not commensurate with the income/net worth of the BO.</i>
6.	<i>Pledge transactions not commensurate with the income/net worth of the BO.</i>
7.	<i>High value off-market transfer immediately after modification of either email ID/mobile number/ address without genuine reason.</i>

8.	<i>Review of reasons for off-market transfer provided by the BO which appears non-genuine based on either profile of the BO or on account of reason codes, including frequent off-market transfer with reason code gift/donation to unrelated parties and/or with reason code off-market sales.</i>
9.	<i>Sudden increase in transaction activity in a newly opened account in a short span of time. An account in which securities balance suddenly reduces to zero and an active account with regular transaction suddenly becomes dormant.</i>
10.	<i>Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.</i>

The above-mentioned alerts will be generated based on some threshold/parameters and are illustrative and not exhaustive. DP have to analyze and review these alerts based on facts and verification of relevant documents including income/net worth as provided by BO. Further, DPs are required to exercise their independent judgment and take appropriate action in order to detect any abnormal or suspicious transactions.

DPs are required to exercise their independent judgment and take appropriate action to detect any abnormal or suspicious transactions. In addition to the above alerts, DPs are expected to generate additional alerts to detect and prevent any type of market manipulation activity carried out by their clients. Also, in case of any abnormal or suspicious activity notice by us then the same will be reported to CDSL/ FIU.

SURVEILLANCE FRAMEWORK FOR DETECTING SUSPICIOUS TRANSACTIONS UNDER RULE 7(3) OF PREVENTION OF MONEY LAUNDERING (MAINTENANCE OF RECORDS) RULES, 2005:

NSBL GROUP has framed its Surveillance Policy to generate alerts as per the indicators provided by FIU in its supplemental guidelines. The generated alerts are analysed with a view to identify suspicious transactions as defined under PML Rules, and if we comes to the conclusion that case appears to be a Suspicious Transaction, then the case shall be brought to the notice of FIU-IND by filing STRs. The alerts are generated on the basis of following criteria:

S. No.	Alert Indicator
1	Account being closed within a short period
2	Off Market sale where consideration value is substantially less than or more than the market value
3	Significant Off-Market Transfer in unsolicited SMS Scrip
4	Suspicious Credit and Debit transactions
5	Off Market Delivery in Unlisted Scrip with more than 1 lakh shares
6	Gift, Donation related Off-Market Transfer where transaction value more than 5times of income range
7	Off Market Transfer with reason code off market sale, gift and donation with value more than 25 lakhs

PROCEDURE ADOPTED FOR ANALYZING THE ALERTS BY SURVEILLANCE TEAM:

1. Alert receipt and Downloading and analyzing alerts:

The alerts provided by exchanges/depositories and the alerts generated at our end are downloaded on daily basis by the Compliance department from respective exchange/Depository system/software for an in depth analysis. The alerts are analyzed based on type of alert, client's past trading pattern, client's occupation, client's financial review, other connected clients in our database, etc. The alerts which are found to be suspicious and of which the Surveillance Team is of the opinion that the same needs to be reported to the exchange/depository are flagged separately. Such alerts are forwarded to the concerned Relationship Manager/Risk Head for further clarification and scrutiny.

2. Due Diligence and investigation

We carry out the due diligence of client(s) on a continuous basis and update all the KYC parameters as prescribed by SEBI and latest information of the client in Unique Client Code (UCC)/BO ID database of the Exchange/Depository.

In order to analyze the trading activity of the Client(s) we establish Group of Client(s)/association amongst clients, inter alia to identify multiple accounts/common accounts/ group of clients to gather relevant information (Transaction logs, client data, etc.) and conduct preliminary investigation and collaborate with internal team and verify alerts with CDSL.

We have an ongoing employee training programme so that the members of the staff are adequately trained in AML/Surveillance obligations and apprising on the Trading Member's surveillance policy. Such training shall have specific focuses for frontline staff, back-office staff, compliance staff, risk management staff and staff dealing with new clients. The said training will conduct at least twice in a year. We set up a separate Surveillance Department / Team consists of:

S.NO	Particulars	Designation
1.	Abhas Jain	Chief Surveillance Officer (CSO)
2.	Abhishek Jain	Director
3.	Tushar Suryavanshi	CTO

3. Alert generation parameters and Processing of alerts:

***NSBL GROUP** has framed its Surveillance Policy to generate alerts as per guidance received from exchanges and depositories from time to time.*

Timelines for responses

- We call for explanation and trading rationale from such identified Client(s)/ Group of Client(s) for entering into such transactions.

- b. We request for documentary evidence such as bank statement/ demat transaction statement or any other documents. In case of funds, we demand for Bank statements of the Client(s)/ Group of Client(s) from which funds pay-in have been met. In case of securities, we request for demat account statements of the Client(s)/ Group of Client(s) from which securities pay-in has been met.
- c. We analyze the documentary evidences, including the bank/ demat statements and record its observations for such identified transactions or Client(s)/ Group of Client(s).
- d. With respect to the transactional alerts downloaded by the exchange/Depository, we ensure that all the alerts are analyzed and status thereof (Verified & closed/ verified & sent to exchange/Depository) including action taken is updated within 45 days, on the member surveillance Dashboard.
- e. With respect to the transactional alerts provided by Depository, we ensure that all alerts are reviewed, and status thereof (Verified & Closed / Verified & Reported to Depository) including action taken is updated within 30 days.
- f. In case, any adverse observations are recorded, we report all such instances to the Exchange/Depository within 45 days of the alert generation by the Exchange/Depository.
- g. With respect to the alerts generated at the DP end, we report instances with adverse observation, along with details of action taken, to CDSL within 7 days of the date of identification of adverse observation
- h. In case of extension is required, we send a request to Exchange/Depository for extension.
- i. If explanation on the same is not satisfactory/ reply not received from the Client within time period as mentioned above then we suspend the client from trading/ report the instance to Regulators (if suspicious).

4. Record Maintenance and review of process:

Each alert received from the Exchange/Depository are backed up by the necessary supporting documentary evidence substantiating the reason for reporting/non reporting the same to the Exchange/Depository.

In case adverse observations are recorded, the Compliance Officer / Chief Surveillance Officer shall report all such instances to the Exchange/Depository within 45 days of the alert generation.

OBLIGATIONS OF COMPLIANCE OFFICER/ CHIEF SURVEILLANCE OFFICER/ DESIGNATED DIRECTOR AND INTERNAL AUDITOR OF THE STOCK BROKING BUSINESS AND DEPOSITORY PARTICIPANT OPERATIONS:

- The surveillance activities of the stock broking operations and that of DP operations shall be conducted under overall supervision of the Compliance Officer / Chief Surveillance Officer of **NSBL GROUP**. The policy implemented by NSBL GROUP in accordance with the provisions of Prevention of Money Laundering Act, 2002 and rules made thereunder as Reporting Entity.
- A quarterly MIS shall be put up by the Compliance Officer / Chief Surveillance Officer to the board and the Designated Director giving number of alerts generated during the quarter, number of alerts closed, number of alerts on which action taken with details of action taken and number of alerts pending at the end of the quarter along with reasons for pendency and action plan for closure. The Board as well as the Designated Director shall be appraised of any exception noticed during the disposal of the alerts.
- The Designated Director shall be responsible for all surveillance activities carried out by the trading member.
- **NSBL GROUP** shall submit its surveillance policy to the internal auditor for stock broking operations and internal auditor of DP operations for review and shall satisfy the queries/questions, if any, raised by the internal auditor with respect to the implementation of the surveillance policy, its effectiveness and the alerts generated.

OBLIGATION OF QUARTERLY REPORTING OF STATUS OF THE ALERTS GENERATED FOR STOCK BROKING OPERATIONS AND DEPOSITORY PARTICIPANT OPERATIONS

- A quarterly statement providing duly approved status of alerts in respect of stock broking operations on quarterly basis shall be submitted to BSE and NSE in the prescribed format within 15 days after the end of the quarter
- A quarterly statement providing duly approved status of alerts in respect of DP operations on quarterly basis shall be submitted to CDSL in the prescribed format within 15 days after the end of the quarter

ESCALATION AND REPORTING MECHANISMS

NSBL shall review the compliance with the provisions of the framework under this Chapter of these regulations not less than once in a quarter and shall verify the adequacy and efficiency of the systems for internal control and reporting by analysing the relevant data.

NSBL are required to inform the details of suspicious activity via email or Member Surveillance Dashboard (MSD) within 48 hours of the detection of suspicious activity.

NSBL shall submit a summary analysis and action taken report on instances of suspicious activity, fraud and market abuse or a 'nil report' where no such instances were detected, on a half-yearly basis to the stock exchanges.

Any deviation in adherence to internal controls, risk management policy, surveillance policy, and policy for onboarding of clients along with the proposed corrective actions for such deviation shall be placed before the appropriate Committee, Board of Directors at regular intervals.

REPORTING OF STATUS OF THE ALERTS GENERATED BY THE Member (NSBL) OR RECEIVED FROM THE EXCHANGES:

1. To the Board of Directors

A quarterly MIS shall be put up to the Board of directors of Nirman Share Brokers Pvt. Ltd. (corporate trading member), in the following format:

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 = C-D)	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	

Reasons for pendency shall be discussed and appropriate action taken. The Board shall be apprised of reasons for pendency and any exception noticed during the disposition of alerts (if any).

2. To the Exchanges -

Trading Members are required to upload the status of the alerts on a quarterly basis to the Exchange within 15 days from the end of the quarter.

Trading members who do not have anything to report, need to submit 'NIL Report' within 15 days from end of the quarter.

ACCOUNTABILITY MATRIX

NSBL shall have an accountability grid for different types of suspicious behavior. A model accountability grid is as under:

Who is being surveilled	Responsibility of trade surveillance on
CEO/Executive Director(s)/Senior Management / Key Managerial Personnel	Board of Directors
Promoters	Board of Directors
Employees	Senior Management/Designated Director
Clients	CSO/Compliance Officer/Designated Director
Authorised Persons	CSO/Compliance Officer/Designated Director

DUTIES AND RESPONSIBILITIES

The Surveillance Policy shall be reviewed on periodic basis and at least once a year by the Compliance Officer / Chief Surveillance Officer to ensure that the same is updated in line with market trends, updated regulations and practices.

This Surveillance policy is approved by the Board of Directors of the Company. The Surveillance process are conducted under overall supervision of the Compliance officer / Chief Surveillance Officer and Designated directors/Compliance officer/ Chief Surveillance Officer are responsible for all surveillance activities carried out by the Company, maintenance of record and reporting of such activities.

This Policy is reviewed by the Internal auditor of the Company and he also ensures its implementation, effectiveness and verifies the alerts generated during the period of audit.

Last reviewed on 01st January 2025