SURVEILLANCE POLICY

Version No: 3

Review date: 30/09/2026
Reviewed By: Compliance Officer

DP SURVEILLANCE POLICY

Introduction:

CDSL vide its Communiqué CDSL/OPS/DP/SYSTM/2021/309 date 15th July 2021 has laid down guidelines pertaining to surveillance obligation of Depository Participant (DP), to facilitate effective surveillance of activities in demat accounts of its clients.

In the said communiqué, CDSL had also stated that DPs shall frame a Surveillance Policy based on nature of DP business, type of accounts, number of demat accounts, transactions done etc.

CDSL, through its Communiqués CDSL/OPS/DP/SYSTM/2024/341 dated June 20, 2024, and CDSL/OPS/DP/SYSTM/2024/552 dated September 20, 2024, has introduced enhanced guidelines on the Surveillance Obligation of Depository Participants (DPs).

Scope:

For the purpose of this Policy 'Beneficiary Owner (BO)' shall mean and include both Individuals and Non-individuals who as on date of this policy have a Demat account with GLOBALWORTH - DP and also all such Individuals and Non-individuals who shall open their Demat Accounts with GLOBALWORTH - DP post framing of this policy.

The Policy has been framed in pursuance of CDSL communiqué on Surveillance Obligations of Depository Participant and applies to those transactions undertaken by BOs in their demat accounts for which alert have been provided by CDSL and also to those transactions for which alerts are generated internally by us, according to parameters set within software which shall be in conformity with at least the minimum standards prescribed by the depository in the above mentioned circular.

The Policy hereinafter defines the following;

1. Broad parameters on basis of which internal alerts are to be generated
2. Review and timeframe for disposal of alerts provided by CDSL & by DP internally
3. Responsibility for closure of alerts
4. Modus-Operandi for investigation, requisition of documents and other subsequent procedures
5. Reporting to CDSL & other authorities as applicable
6. Escalation Matrix and actions for non-cooperation by clients.
7. Reporting of Alerts & their disposition to Board of Directors & Depositories
8. Obligations of Compliance Officer & Internal/Concurrent Auditors
9. Miscellaneous Matters related to Surveillance Activity.

As per CDSL Communiqués, it is mandatory to have in place appropriate Surveillance Policies and Systems to detect, monitor and analyze transactions.

Hence, we have to co-relate the transaction data with BO's information/data and detect suspicious/manipulative transactions. It will be an ongoing continuous process with analysis of trades and transactions. Further, we are required to carry out Client Due Diligence (CDD) on a continuous basis.

1. Broad Parameters for internal generation of alerts :

Depository will provide us alerts as mentioned in the communiqué which have to be downloaded by us. In addition to this, GLOBALWORTH - DP shall generate alerts on their in-house surveillance software which shall be as under:

- Multiple Demat accounts opened with same demographic details, with same PAN, Mobile Number, Email ID, Bank Account nos. etc. considering the existing demat accounts held with us.

- BOs whose e-mails sent on registered e-mail ID are bounced back

- BOs whose letters/documents sent to their addresses registered with us are returned undelivered

- Frequent changes in details of BO especially in Address, Mail ID, Mobile number, Authorised Signatories, POA holder etc.

- Disproportionate transactions &/or holdings v/s reported Annual income / Net worth.

- Frequent Off-market transfers by BO in a specified period

- Off-market transfers & Pledge transactions that do not commensurate with the Annual Income / Net-worth of the client

- High value off-market transactions immediately after modification of client master details in any account

- Review of reasons given for off-market transfers by BO vis-à-vis BO's profile for
  e.g. frequent transfers with consideration or gifts/donations to unrelated parties

- Newly opened demat accounts where there is sudden increase in transactions activities in short span of time and suddenly holdings becoming zero or account remaining dormant after some time

- Any other alerts & mechanism in order to prevent & detect any type of market manipulation activity carried out by BOs

2. Time-frame for investigation & closure of Alerts

Step	Process	Timeframe
1. Alert Generation	Alerts generated by CDSL or DP's internal system.	T (Day of alert generation)
2. Preliminary Review	Surveillance Team reviews the alert, assesses risk, and determines if further investigation is required.	T+3 Days
3. Client Communication	If necessary, BO is contacted for an explanation and supporting documents.	T+7 Days
4. Follow-up & Escalation	If no response from BO, a follow-up is initiated. If still unresponsive, the case is escalated to Compliance Officer.	T+15 Days
5. Review & Verification	Documents received from BO are reviewed, and transactions are validated against KYC details.	T+25 Days
6. Alert Closure/Reporting	If no discrepancies are found, the alert is marked as closed. If suspicious activity is detected, the alert is reported to CDSL.	T+28 Days
7. Board Reporting	Alerts and dispositions are reported to the Board in the quarterly MIS.	End of Quarter

3. Responsibility for closure of alerts

All alerts generated internally shall be closed as per time-frame mentioned in point no 2 above. Alerts received from Depositories shall be closed by Compliance Team on the respective portals.

The responsibility for investigating alerts received from CDSL lies with the compliance officer. Surveillance department headed by the compliance officer will be primarily responsible for investigation, requisitioning documents & follow up, if any. Accordingly they will make their observations & close/report the alerts.

Surveillance team shall also be responsible for investigating internal generated alerts and shall report to the Compliance Team of any adverse findings

4. <u>Modus-operandi for investigation, requisition of documents and other subsequent procedures</u>.

4.1. Analysis of alerts: - Surveillance Team shall analyze transactions on basis of alerts received from CDSL and internal system. Points to be considered while analyzing transactional alerts are

a) Income Range / Net worth declared by the BO as against transactions done or holdings in the account

b) Verification of Ultimate Individual Beneficial owners in case of Non-Individual BOs.

c) Verification of source & destination of off-market debits & credits in BO's account

d) Verification of family, background etc where same demographic details, Mail ID,
Mobile numbers are used in multiple accounts

e) Verification of addresses in case of documents returned undelivered

f) Review of reasons given for off-market debits

g) Wherever required additional relevant documents shall be requested from BO client for analyzing alerts.

h) Scrutiny of explanations and documents furnished by BO against alerts received on their transactions.

4.2 Updating of Client(s) Information/ Due diligence measures:

a) For any BO or group of BOs for whom alerts have been trigged multiple times –

- Client Due diligence shall be carried out on an on-going basis.
- KYC parameters of BOs shall be updated on a periodic basis and latest information shall be updated in the CDAS

b) BOs shall be advised to update their Annual Income &/or Net-worth as and when necessary especially where BO's transactions/holdings do not commensurate with existing Annual Income &/or Net-worth.

c) For this purpose, BOs with Transactions or Holdings exceeding 1.5 times of Net- worth shall have to re-furnish the information to us.

d) Stricter Monitoring for Anomalous Transactions:
- Additional verification for multiple demat accounts linked to the same bank account.
- Scrutiny of accounts opened using multiple PANs by a single entity.
- CDSL has imposed monetary penalties and account restrictions for non-compliance.

5. Escalation Matrix and actions for non-cooperation by clients.

a) In the event of any BO not furnishing requisite details or explanation as requested by DP, the matter shall be escalated to CEO/Director under recommendation of Compliance Head.

b) In case of BO does not furnish or is not co-operative to furnish requisite document/information within time-frame given, all further requests & debit transactions in the BO account shall be suspended alongwith freeze of BO's trading account. BO shall be intimated about suspension of activities in his demat account through e-mail/SMS.

6. Reporting of Alerts & its disposition

a) Quarterly MIS shall be put forth to Board of Directors within 7 days from end of each quarter as under:

- Number of alerts pending at the beginning of the quarter
- Number of alerts generated during the quarter
- Number of alerts processed & closed during the quarter
- Number of alerts pending at end of the quarter with reasons for pendency & action plan for closure
- Any exceptions noticed during disposal of the alerts

b) Duly approved status of the alerts on a quarterly basis shall be provided to CDSL as per their format given below or any other format provided at a later date within 15 days from end of the quarter. In case there is nothing to report, then a NIL report shall have to be submitted to the depositories.

Status of Alerts generated by the Depository:

Name of Alert	No. of alerts pending at beginning of quarter	No. of new alerts generated during the quarter	No. of alerts verified & closed in the quarter	No. of alerts reported to Depository	No. of alerts pending process at the end of the quarter

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

Sr. No.	Brief action taken during the quarter

C. Enhanced Quarterly Reporting Format:

- Additional columns introduced for comprehensive tracking of alerts.
- Aging analysis of pending alerts with categorized reasons for pendency.
- Mandatory alignment of opening and closing balances between quarters.
- The new format is effective September 30, 2024.

D. New Online Submission Process for Quarterly Reports:

- Submission through CDSL Surveillance Portal with step-by-step reporting:
  - Select "Quarterly Reporting" under "Alert Reporting by DP".
  - Choose the appropriate alert type and enter required details.
  - Provide reasons for all pending alerts.
  - Ensure total counts match across sections.
  - Submit the report before the 15th of the month following the end of the quarter.

7. Obligations of Compliance Officer & Internal/Concurrent Auditors

- DP Surveillance activity shall be conducted under overall supervision of Compliance Officer

- Internal Auditor of DP shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the Audit period. The Auditor shall record the observations with respect to the same in their report

- Internal Auditor shall verify that the quarterly MIS is prepared & placed before the Board of Directors

8. Miscellaneous Matters in connection with Surveillance Activity

8.1. Record Maintenance:

The records for all alerts and related documents shall be maintained for a period of 10 years as specified under the Prevention of Money Laundering Act.

8.2. Regulatory Penalties:

- During Inspection, if it is observed that DP has not fulfilled their Surveillance obligation then appropriate disciplinary action shall be initiated by CDSL against the DP. Hence, as a responsible intermediary, GLOBALWORTH - DP has to ensure timely analysis & reporting of alerts.

- In event of any penalty being levied by depositories for transactions deemed abnormal/ non-genuine, the Compliance Head shall, in consultation with Management, issue show cause notice to the concerned BOs calling for explanation as to why penalties should not be passed onto them or other suitable action not be initiated against them.

- In the event of failure on part of the BOs to respond to aforesaid show cause notice within the prescribed time, Compliance Head shall initiate necessary action for recovery of the penalty amount including but not limited sale of shares, suspension/closure of trading & demat accounts or any other action as may be deemed necessary.

8.3. Policy Review:

- An event based review of this Policy shall be done on the basis of any regulatory updates and/ or improvisation in process of investigation of alerts.

- Every change in the procedure and new norms introduced by regulatory authorities shall be communicated by Compliance team and incorporated in the policy.

- Regular training to be conducted to surveillance team for ensuring the compliance of the said circular.