SEBI Registration number: INZ000261035 (Stock Broker)

NSE Member ID: 06433

SEBI Registration No: IN301372 (NSDL)

POLICY ON : Standard Operating Procedure (SOP) for handling Cyber Security incidents

Registered Office: 86, Canning Street, Kolkata-700001

Compliance Officer: Mr. Surya Prakash Lunia
E-Mail Id: complianceofficer@daulatsec.com

Principal Officer:
Surya Prakash Lunia
E-Mail Id: complianceofficer@daulatsec.com

Designated Officer-Jitendra Kochar
E-Mail Id: jitenko@hotmail.com

Release Date: 08-11-2024
Version: 2.0

Standard Operating Procedure (SOP) for Processing Surveillance Alerts

1. Objective

This SOP outlines the process for handling surveillance alerts generated at the Depository Participant (DP) end as well as those generated by National Securities Depository Limited (NSDL). The aim is to ensure timely and effective monitoring and management of client transactions to comply with regulatory requirements.

2. Scope

This SOP applies to all surveillance alerts generated by the SBSBL or provided by NSDL. It includes the procedures for alert generation, processing, escalation, and resolution.

3. Responsibilities

- **Compliance Officer:** Responsible for periodic review of this SOP and ensuring adherence to the procedures.
- **Surveillance Team:** Responsible for processing alerts, including their generation, review, and disposal within specified timelines.
- **Designated Maker-Checker Roles:** Maker and Checker mechanism has been implemented to check and verify the closure of alerts.

4. Alert Generation Parameters

Alerts are generated based on specific triggers or parameters set within the DP's system or provided by NSDL based on the following criteria:

SN	Particular
1.	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.
2.	Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
3.	Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.
4.	Frequent Off-Market transfers by a client in a specified period
5.	Off-market transfers not commensurate with the income/Networth of the client.
6.	Pledge transactions not commensurate with the income/Networth of the client.
7.	Off-market transfers (High Value) immediately after modification of details in demat account
8.	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
9.	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.

5. Timelines for Response

- With respect to the transactional alerts provided by Depository, DP shall ensure that all alerts are reviewed, and status thereof (Verified & Closed / Verified & Reported to Depository) including action taken is updated within 30 days.
- With respect to the alerts generated at the DP end, DP shall report instances with adverse observation, along with details of action taken, to CDSL within 7 days of the elate of identification of adverse observation. Further DP shall ensure that all alerts are reviewed, and status thereof (Verified & Closed / Verified & Reported to Depository) including action taken is updated within 30 days.
- Alerts pending beyond the stipulated timeframe must be escalated as per the escalation matrix.

6. Escalation Procedures

In the event of delays or unresolved alerts, the following escalation steps should be followed:

1. **Day 20:** Initial reminder sent to the surveillance team.
2. **Day 25:** Escalation to the Compliance Officer.
3. **Day 30:** Final escalation to senior management with details of the pending alerts.

7. Alert Processing and Disposal

- **Maker-Checker Mechanism:** A dual control process shall be followed where one individual (Maker) initiates the action on the alert, and another individual (Checker) reviews and approves the action.
- Alerts must be categorized, analyzed, and appropriate actions must be documented.
- The closure of alerts must be documented with reasons, and all supporting evidence should be attached to the alert record.

8. Periodic Review

- The SOP and alert generation parameters must be reviewed at least once a year by the Compliance Officer.
- Amendments to the SOP should be made based on changes in regulatory requirements, identified gaps, or improvements in alert handling processes.

9. Documentation and Reporting

- All alerts and actions taken should be documented in the prescribed format.
- A quarterly report on the status of alerts, including the number of alerts generated, closed, and pending, must be submitted to NSDL as per the new format.

10. Non-Compliance and Disciplinary Actions

- Any non-compliance with this SOP, including delays in processing alerts or repeated lapses in reporting, may result in disciplinary actions as per the DP Operating Instructions and NSDL bye-laws.