(Member: BSE, NSE, MSEI, MCX, Depository Participant of NSDL & CDSL)
Corporate Off.: 303, New Delhi House, 27, Barakhamba Road, New Delhi-110001
Phones: 011 43074307, CIN: U74899DL1995PTC070418
Website: www.integratedmaster.com; Email id: compliance@integratedmaster.com

SURVEILLANCE POLICY FOR DEPOSITORY PARTICIPANTS (DP) OPERATIONS

Policy Creation Date: **18th September, 2021**
Version Number: **1.0**
Subsequent Revision Dates: **07th September, 2024; 27th May, 2025; 25th June, 2025**
Approved By: **Board**

Applicability:

The policy is framed in accordance with the provision of SEBI Circular No. SEBI/HO/ISD/ISD/CIR/P/2021/22 dated 01.03.2021, CDSL communique No. CDSL/OPS/DP/SYSTM/2021/309, dated 15.07.2021/ COMMUNIQUÉ no. CDSL/OPS/DP/SYSTM/2024/341 dt. June 20, 2024. The said policy has been approved by the Board of Directors in Board Meeting held at the Registered office of the company on **25.06.2025**.

In order to further strengthen the Surveillance framework for the Securities Market, Depository Participant is hereby advised to put in place a surveillance framework, which shall cover the following: -

What is Surveillance?

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. In order to ensure investor protection and to safeguard the integrity of the markets, it is imperative to have in place an effective market surveillance mechanism. The main objective of the surveillance function is to help maintain a fair and effective market for securities.

Therefore, we have decided to undertake adequate measures for ensuring effectiveness and efficiency of the trading and depository system. The Company with the above motive in mind has framed Surveillance policy focusing on:

- To establish a surveillance mechanisms and controls in the operations /trading activity.
- To put in place appropriate controls for the detection and reporting of suspicious trading activities in accordance with applicable laws/laid down procedures.
- To comply with applicable laws and regulatory guidelines.

Surveillance Policy for operations as Depository Participant: -

Depository Participant is providing transactional alerts on quaterly basis based on threshold defined by NSDL / CDSL to the all the DPs report download utility. As per applicable Circular, the company 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 provisions of PMLA (Maintenance of records) Rules,2005.

In addition to the same, company has identified various Surveillance parameters in respect of its operations as Depository Participant to generate alerts as per guidance provided in NSDL / CDSL Circulars based on following criteria:

- 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.

- Email/ letters sent to clients on their registered email ID/address which bounces/ returns undelivered.

- 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.

- Frequent off-market transfer of securities more than twice in a month without genuine reasons.

- Off-market transactions not commensurate with the income/ Networth of the BO.

- Pledge transactions not commensurate with the income/Networth of the BO.

- High value off-market transfer immediately after modification of either email ID/mobile number/ address without genuine reason.

- 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.

- 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.

Obligation of Depository Participant to frame Surveillance Policy:

Integrated Master Securities Pvt. Ltd. has framed a surveillance policy based on nature of depository business, type of clients, number of Demat accounts, number of transactions etc. which, inter alia, cover the following: -

- Generation of suitable surveillance alerts which may be guided by indicative themes.
- Documentation of reasons for delay, if any, in disposition of alerts.
- Framework of appropriate actions that can be taken by the Participant as per obligations under PMLA.
- Disposal of alerts within 30 days from the date of alerts generated at Participants end and alerts provided by NSDL/CDSL. Documentation of reasons for delay, if any, in disposal of alerts.
- Reporting to NSDL/CDSL and other authorities as applicable in case of any abnormal activity.
- Review and disposal of transactional alerts provided by NSDL/CDSL. However, Integrated Master Securities Pvt. Ltd may describe its own parameters to generate additional alerts of their own.
- Record maintenance for the period as stipulated under applicable statutes.
- The surveillance policy of the Participants shall be reviewed once in a year.

Key Surveillance Mechanisms:

Transaction Surveillance:

- Monitoring high-value or unusual off-market transactions
- Identification of sudden or large demat/remat requests
- Scrutiny of transfers involving dormant or recently activated accounts

Pattern Detection:

- Alerts for circular transfers, rotation of securities
- Multiple accounts with similar credentials (email, mobile, address)
- Irregularities in pledging/unpledging transactions

Preparation of SOP for Alert Generation and Disposal:

A Standard Operating Procedure (SOP) shall be documented for:

- Generating meaningful alerts using internal surveillance systems/back-office tools.
- Categorizing alerts as Low/Medium/High risk.
- Defining timelines and responsibilities for investigation and disposal.
- Escalating unresolved or significant alerts to higher authorities

Segregation of Duties (Maker & Checker Concept):

To ensure checks and balances:

Entry of Transaction Alerts must be initiated by the Maker.

Independent verification and authorization to be performed by a Checker

Dual-control processes to be enforced for sensitive activities such as

pledge marking, remat, and bulk transfers.

Staff Training & Awareness:

Ongoing training programs and seminars on Depository operations will be conducted to:

- Educate staff on regulatory requirements and red flags
- Reinforce importance of segregation of duties and surveillance obligations
- Equip staff with skills to interpret alerts and apply SOPs

Reporting to the Board and Committees:

A quarterly surveillance report will be presented to:

- The Board of Directors
- The Audit Committee or Risk Management Committee, if constituted

The report shall cover:

- Summary of alerts generated and disposed
- Trends and observations
- Name of Alert
- Opening balance of Alerts at the beginning of Quarter
- No of alerts generated during the quarter
- Total No of Alerts
- No. of Alerts closed during the quarter
- Alerts pending at the end of quarter
- Ageing analysis of the alerts pending at the end of the quarter (since alert generation date)
- Reasons for pendency

Client due diligence (CDD):

The CDD measures comprise the following: -

- Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

- Verify the client's identity using reliable, independent source documents, data or information.

- Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted.

- Verify the identity of the beneficial owner of the client and/or the person

on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c).

- Understand the ownership and control structure of the client.

- Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary' s knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;

- Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

- Participant will carry out the Due Diligence of their client(s) on an on-going basis.

- Participant shall ensure that key KYC parameters of the clients are updated on a periodic basis as prescribed by SEBI and latest information of the client is updated in Depository System.

Reliance on third party for carrying out Client Due Diligence (CDD):

- Integrated Master Securities Pvt. Ltd should rely on a third party for the p u r p o s e of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligation s under the PML Act.

- Such reliance shall be subject to the conditions that are specified in Rule 9
(2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

Safeguards on Acceptance of clients:

The following safeguards are to be followed while accepting the clients:-

No account is opened in a fictitious / benami name or on an anonymous basis. To ensure this we must insist the client to fill up all the necessary details in the KYC form in our presence and obtain all the necessary documentary evidence in support of the information filled in KYC. We identify the client whether he is debarred entity or not?

We must verify all the documents submitted in support of information

filled in the KYC form with the originals and in-person verification should be done by our own staff.

In case we have any doubt that in-complete / fictitious information is submitted by the client, we must ask for such additional information so as to satisfy ourselves about the genuineness of the clients.

We should not continue to do business with such a person and file a suspicious activity report. We should also evaluate whether there is suspicious trading in the account and whether there is a need to freeze or close the account.

We should be careful while accepting clients of special category like NRIs, HNIs, Trust, Charities, NGOs, Politically Exposed Persons (PEP), persons of foreign origin, companies having closed shareholding/ ownership, companies dealing in foreign currency, overseas in high-risk countries, non-face to face clients, clients with dubious background. Current/Former senior high-profile politician, Companies offering foreign exchange, etc.) or clients from high-risk countries or clients belonging to countries where corruption/fraud level is high. Scrutinize minutely the records/documents pertaining to clients belonging to aforesaid category.

Alerts based on New typologies:

Integrated Master Securities Private Limited is committed to continuously strengthening its surveillance framework by integrating alerts arising from emerging risk typologies identified by:

SEBI, Depositories (NSDL/CDSL), Financial Intelligence Unit (FIU-IND), Internal findings or audits, Market-wide incidents or trends.

Following alerts are generated by the Depository Participant's back office surveillance system:

S.No	PARTICULARS OF ALERTS
a.	Multiple Demat Accounts Opened with same demographic details.
b.	Alert for communication sent on registered Email id/address of clients are getting bounced.
c.	Frequently changes in client masters
d.	Frequent Off-Market transfers by a client
e.	Off-market transfers not commensurate with the income/Networth of the client
f.	Pledge transactions not commensurate with the income/Networth of the client
g.	Off-market transfers (High Value) immediately after modification of details in demat account
h.	Frequent transfers with reason code Gifts/Donation/Off Market Sale to unrelated parties
i.	Alert for newly opened accounts and suddenly holding in demat account becomes zero.
j.	Off Market transfer to UnRelated Accounts
k.	Suspecious off market credit and debit
l.	Off market delivery in unlisted scrip
m.	Gift Donation Related Off Market Transfer

n.	Off market transfer at variance with market value
o.	Off market transfer in suspecious scrip
p.	Suspecious Closure of Account

Processing of Alerts:

Integrated Master Securities Pvt. Ltd. will process the Alerts in the following manner:-

- Integrated Master Securities Pvt. Ltd will maintain register (electronic/physical) for recording of all alerts generated.

- While reviewing alerts, Participant shall obtain transaction rationale, verify demat account statement and also obtain supporting documents as required from the client.

- After verifying the documentary evidences, Participants shall record its observations for such identified transactions of its Client.

- Transactional alerts to be provided by Depository, Participants shall ensure that all alerts are reviewed and status thereof (Verified & Closed/Verified & Reported to Depository) including action taken is updated within 30 days, on the NSDL e-PASS portal. The procedure w.r.t sharing of alert by NSDL/CDSL with Participants and report submission by Participants in this regard will be provided separately.

- With respect to the alerts generated at the Participant end, participant shall report instances with adverse observation, along with details of action taken, to NSDL/CDSL within 7 days of the date of identification of adverse observation.

- The designated officials who are tasked to review the alerts on daily basis shall review the same.

- If the designated official finds after review and due diligence that the alert is required to be closed, the official shall close the same with appropriate remarks.

- The records of alerts generated, disposed of as closed and details of action taken wherever applicable shall be maintained 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.

- The Compliance Officer, after review of the alerts along with the submitted comments of the designated official, decides to close the alert, he/she shall close it with appropriate remarks. If the Compliance Officer finds that action in respect of such alert is warranted, he/she shall take such actions including filing STR with FIU-India, informing NSDL/ CDSL and/or discontinue the relationship with the client.

Obligation of Compliance officer and Internal Auditor/ Concurrent

Auditor of the Participants:

- The surveillance activities of DP operations shall be conducted under overall supervision of the Compliance Officer.

- The policy implemented 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 to the Board on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with reasons for pendency and action plan for closure.

  Also, the Board shall be apprised of any exception noticed during the disposal of alerts.

- Internal auditor of Participant shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.

- Internal Auditor shall verify that the quarterly MIS is prepared and placed before the Board of the Participant.

REPORTING OF ALERTS:

The Company shall provide duly approved status of the Alerts on a Quarterly basis to the exchange in the format prescribed by the exchange within 15 days from the end of the quarter.

In case zero alert during the quarter, NIL report need to be submit to the exchange as per the prescribed format.

As per COMMUNIQUÉ no. CDSL/OPS/DP/SYSTM/2024/341 dt. June 20, 2024, DPs are required to generate appropriate surveillance alerts at their end, to enable them to effectively monitor the transactions of their clients at their end as per the laid down surveillance policy. Further DP has obligation of reporting the status of alerts generated to CDSL in the below 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	3-6months	>6 months	

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

In case "Integrated Master Securities Pvt. Ltd." does not have anything to

report, a "NIL Report" shall be filed within 15 days from the end of the quarter. The above format will come in effect from September 30, 2024.

Appropriateness of Resources for Surveillance:

Integrated Master Securities Private Limited recognizes that an effective surveillance framework requires adequate and appropriate resources. The following measures ensure that surveillance operations are well-supported:

Human Resources:

- *Qualified Personnel*: Dedicated and trained staff are appointed to oversee surveillance activities, including alert generation, investigation, and escalation.

- *Segregation of Roles*: Roles are clearly defined, with separation of duties between operations (maker), compliance (checker), and audit (review).

- *Staffing Levels*: Adequate staffing is maintained based on the scale of operations and volume of transactions.

- Technology & Systems:

  Surveillance Tools: Use of reliable and updated back-office and surveillance systems that can generate meaningful alerts based on pre-defined risk parameters.

  Automation: Emphasis on automation to reduce manual errors and improve efficiency in monitoring and report generation.

  System Capacity: Systems must be capable of handling the volume of DP transactions without delay or data loss.

- Infrastructure:

  Secure Environment: Surveillance data is stored in secure, access-controlled systems to ensure confidentiality and integrity.

  Redundancy & Backup: Proper IT infrastructure is in place to ensure uninterrupted monitoring, even in cases of primary system failure.

  Logical Actionables for Material or High-Risk Alerts:

  Material or high-risk alerts identified through surveillance systems or manual processes must be addressed through a structured and time-bound escalation and response mechanism. The following logical and actionable steps shall be followed:

  Initial Review and Documentation:

  Each material/high-risk alert must be:

  • Reviewed immediately by the Compliance Officer or designated

surveillance personnel.
• Recorded in the alert management system with a unique reference number and timestamp.
• Classified based on nature (e.g., off-market transfer anomaly, pledge misuse, multiple demats, etc.).

Preliminary Investigation:

The Compliance team shall:

• Verify the underlying transaction(s) and account activity.
• Check the client's historical behavior and KYC records.
• Cross-check with other internal departments (operations, KYC, etc.) as necessary.

Escalation:

If the alert is found to have potential for misuse, market manipulation, or regulatory breach:

• Immediately escalate to the Principal Officer, Head of Compliance, or Risk Committee.
• Consider temporary blocking of further transactions in the affected account if required under policy provisions.
• Alert the depository (NSDL/CDSL) in cases of suspected fraud or system misuse.

Client Engagement:

If appropriate and without compromising any ongoing investigation:

• The client may be contacted to provide justification or documentation related to the suspicious activity.
• All communication with the client shall be recorded.

Final Decision and Reporting:

The alert is closed or confirmed based on findings.

• If found suspicious:

• File a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU-IND), if required.

• Inform the relevant depository and SEBI as applicable.

• Maintain full documentation of the investigation, including actions taken, persons involved, and closure status.

Board/Committee Reporting:

Material alerts and their resolution status shall be:

Included in the quarterly surveillance report to the Board or Audit/Risk

Management Committee.

Highlighted if the issue posed significant financial, reputational, or compliance risk.

Post-Incident Review:

In case of repeated high-risk alerts from a particular client, segment, or staff operation:

• Conduct a root cause analysis.

• Implement corrective measures, such as system rule enhancement, re-training of staff, or KYC re-verification of the client.

Review of Policy:

The Surveillance Policy of the participants shall be reviewed once a year which is presented and reviewed by Board of Directors at Board Meeting dated 27.05.2025 to ensure that the same is updated in line with market trends, updated regulations.

For and on behalf of
Integrated Master Securities Private Limited

S. C. Khaneja
Director
(DIN: 00042758)

Integrated Master Securities Pvt Ltd
(Member: BSE, NSE, MSEI, MCX, Depository Participant of NSDL & CDSL)
Corporate Off.: 303, New Delhi House, 27, Barakhamba Road, New Delhi-110001
Phones: 011 43074307, CIN: U74899DL1995PTC070418
Website: www.integratedmaster.com;Email Id:compliance@integratedmaster.com

---

Standard Operating Procedure (SOP) for DP Surveillance Alerts Generation and Processing

SOP Creation Date: **18th September, 2021**
Version Number: **1.0**
Subsequent Revision Dates: **07th September, 2024; 27th May, 2025; 25th June, 2025**
Approved By: **Board**

Objective:

The objective of this policy is to have in place an effective surveillance mechanism to ensure investor protection and to safeguard the integrity of the markets. The goal of surveillance is to spot adverse situations and to pursue appropriate preventive actions to avoid disruption. The aim is to ensure timely and effective monitoring and management of client transactions to comply with regulatory requirements.

Scope:

This procedure applies to all surveillance activities related to DP transactions, covering the generation, review, and resolution of alerts.

Responsibilities:

- Compliance Officer: Responsible for periodic review of this SOP and ensuring adherence to the procedures.
- IT Support: Maintains and updates the surveillance system.
- Surveillance Team: Responsible for monitoring and analysing alerts.
- Designated Maker-Checker Roles: Maker and Checker mechanism has been implemented to check and verify the closure of alerts.
- Senior Management: Oversees the effectiveness of the surveillance process.

Alert Generation:

- The backened SHILPI Software Version No-16.00 Build: 18120 automatically generates alerts based on predefined rules and thresholds set by regulatory bodies and internal risk management teams.

- Alert Generation Parameters include:
    - Alert for multiple demat accounts opened with same demographic details.
    - Alert for communication sent on registered Email id/address of clients are getting bounced.
    - Frequent changes in the details of the demat accounts.
    - Frequent Off-Market transfers by a client.
    - Off-market transfers not commensurate with the income/Networth of the client.
    - Pledge transactions not commensurate with the income/Networth of the client.
    - Off-market transfers (High Value) immediately after modification of details in Demat account.
    - Reason of Off Market transfers not matching with Client profile.
    - Sudden increase in Transactions and holding becomes zero in New accounts.
    - Off Market transfer to Unrelated Accounts.
    - Gift Donation Related Off Market Transfer.
    - Off Market Transfer at Variance with Market Value.
    - Off Market Transfer in suspicious scrip.
    - Account Opened and Quickly Closed.
    - High Volume/Value Dematerialization Alerts.
    - Transaction in Dormant Account.
    - High Volume/Value Preferential Allotment.
    - Significant Holding in Listed Scrip.
    - High Value Credit/ High Quantum Credit / High value Gift or Donation Credit.
    - High Value Debit / High Quantum Debit / High value Gift or Donation Debit.

Alert Review Process

Step 1: Initial Screening

o The Surveillance Team reviews alerts in the system.

o Basic checks include transaction type, client profile, and historical patterns

Step 2: Detailed Analysis

- o Additional scrutiny is applied to high-risk alerts.
- o Supporting documents and client interactions are reviewed.

Step 3: Escalation

- o If suspicious activity is confirmed, the alert is escalated to the Compliance Team.
- o Compliance may conduct further investigation or request additional information.

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.

Resolution & Closure

• Alerts are categorized as:

- o False Positives: Closed with documentation.
- o Genuine Alerts: Escalated for further action.

• Compliance Team documents findings and, if required, reports the case to regulatory authorities.
• Closure of alerts is logged with appropriate remarks and supporting evidence.

Reporting & Record Keeping

• All alerts, actions taken, and resolutions are documented and stored securely.
• Periodic reports are generated for review by senior management.
• Regulatory reports are filed as per compliance requirements.

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.
System Maintenance & Review
• Regular updates and enhancements to alert parameters are conducted based on trends and regulatory changes.
• Periodic audits ensure the efficiency and effectiveness of the surveillance process.

Training & Awareness

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

Compliance & Regulatory Requirements

• Adherence to guidelines issued by regulatory bodies such as SEBI and Stock Exchanges.
• Periodic compliance audits and self-assessments.

Exception Handling

• Any deviations from the SOP must be documented and approved by senior management.
• Emergency measures can be implemented in case of system failures or significant security threats.

This SOP ensures a structured approach to DP surveillance, enhancing regulatory compliance and mitigating risks associated with fraudulent or suspicious transactions.

For and on behalf of

Integrated Master Securities Private Limited

S. C. Khaneja
Director
(DIN: 00042758)

xxxxxxxxxxxx
xxxxx

Integrated Master Securities Pvt Ltd
(Member: BSE, NSE, MSEI, MCX, Depository Participant of NSDL & CDSL)
Corporate Off.: 303, New Delhi House, 27, Barakhamba Road, New Delhi-110001
Phones: 011 43074307, CIN: U74899DL1995PTC070418
Website: www.integratedmaster.com;Email Id:compliance@integratedmaster.com

Standard Operating Procedure (SOP) for DP Surveillance Alerts Generation and Processing

SOP Creation Date: **18th September, 2021**
Version Number: **1.0**
Subsequent Revision Dates: **07th September, 2024; 27th May, 2025; 25th June, 2025**
Approved By: **Board**

Objective:

The objective of this policy is to have in place an effective surveillance mechanism to ensure investor protection and to safeguard the integrity of the markets. The goal of surveillance is to spot adverse situations and to pursue appropriate preventive actions to avoid disruption. The aim is to ensure timely and effective monitoring and management of client transactions to comply with regulatory requirements.

Scope:

This procedure applies to all surveillance activities related to DP transactions, covering the generation, review, and resolution of alerts.

Responsibilities:

- Compliance Officer: Responsible for periodic review of this SOP and ensuring adherence to the procedures.
- IT Support: Maintains and updates the surveillance system.
- Surveillance Team: Responsible for monitoring and analysing alerts.
- Designated Maker-Checker Roles: Maker and Checker mechanism has been implemented to check and verify the closure of alerts.
- Senior Management: Oversees the effectiveness of the surveillance process.

Alert Generation:

- The backened SHILPI Software Version No-16.00 Build: 18120 automatically generates alerts based on predefined rules and thresholds set by regulatory bodies and internal risk management teams.

- Alert Generation Parameters include:
    - Alert for multiple demat accounts opened with same demographic details.
    - Alert for communication sent on registered Email id/address of clients are getting bounced.
    - Frequent changes in the details of the demat accounts.
    - Frequent Off-Market transfers by a client.
    - Off-market transfers not commensurate with the income/Networth of the client.
    - Pledge transactions not commensurate with the income/Networth of the client.
    - Off-market transfers (High Value) immediately after modification of details in Demat account.
    - Reason of Off Market transfers not matching with Client profile.
    - Sudden increase in Transactions and holding becomes zero in New accounts.
    - Off Market transfer to Unrelated Accounts.
    - Gift Donation Related Off Market Transfer.
    - Off Market Transfer at Variance with Market Value.
    - Off Market Transfer in suspicious scrip.
    - Account Opened and Quickly Closed.
    - High Volume/Value Dematerialization Alerts.
    - Transaction in Dormant Account.
    - High Volume/Value Preferential Allotment.
    - Significant Holding in Listed Scrip.
    - High Value Credit/ High Quantum Credit / High value Gift or Donation Credit.
    - High Value Debit / High Quantum Debit / High value Gift or Donation Debit.

Alert Review Process

Step 1: Initial Screening

o The Surveillance Team reviews alerts in the system.

o Basic checks include transaction type, client profile, and historical patterns

Step 2: Detailed Analysis

- o Additional scrutiny is applied to high-risk alerts.
- o Supporting documents and client interactions are reviewed.

Step 3: Escalation

- o If suspicious activity is confirmed, the alert is escalated to the Compliance Team.
- o Compliance may conduct further investigation or request additional information.

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.

Resolution & Closure

• Alerts are categorized as:

- o False Positives: Closed with documentation.
- o Genuine Alerts: Escalated for further action.

• Compliance Team documents findings and, if required, reports the case to regulatory authorities.
• Closure of alerts is logged with appropriate remarks and supporting evidence.

Reporting & Record Keeping

• All alerts, actions taken, and resolutions are documented and stored securely.
• Periodic reports are generated for review by senior management.
• Regulatory reports are filed as per compliance requirements.

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.
System Maintenance & Review
• Regular updates and enhancements to alert parameters are conducted based on trends and regulatory changes.
• Periodic audits ensure the efficiency and effectiveness of the surveillance process.

Training & Awareness

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

Compliance & Regulatory Requirements

• Adherence to guidelines issued by regulatory bodies such as SEBI and Stock Exchanges.
• Periodic compliance audits and self-assessments.

Exception Handling

• Any deviations from the SOP must be documented and approved by senior management.
• Emergency measures can be implemented in case of system failures or significant security threats.

This SOP ensures a structured approach to DP surveillance, enhancing regulatory compliance and mitigating risks associated with fraudulent or suspicious transactions.

For and on behalf of

Integrated Master Securities Private Limited

S. C. Khaneja
Director
(DIN: 00042758)

xxxxxxxxxxxx
xxxxx