Policy on Standard Operating Procedures for Depository Participant Surveillance Activities

1. Purpose

The purpose of this policy is to establish a clear and consistent framework for the surveillance activities of Depository Participants (DPs) to ensure compliance with regulatory requirements, maintain operational efficiency, and mitigate risks.

2.Scope

This policy applies to all employees, all client(s), departments, and activities involved in the surveillance of DPs, including transaction monitoring, compliance checks, and risk management.

3.Policy Statement

The organization is committed to implementing and maintaining comprehensive standard operating procedures (SOPs) for the surveillance of DPs. These SOPs aim to detect, analyze, and report any suspicious or non-compliant activities to ensure the integrity and security of the depository system.

4.Definitions

- Depository Participant (DP): An agent of the depository through which it interfaces with the investors.
- Surveillance: The process of monitoring the activities of DPs to ensure compliance with regulations and internal policies.
- Standard Operating Procedures (SOPs): Detailed, written instructions to achieve uniformity of the performance of a specific function.

5. Roles and Responsibilities

- Compliance Officer: Ensure adherence to regulatory guidelines and internal policies.
- Surveillance Team: Monitor activities, analyze data, and report irregularities.
- IT Team: Maintain and support surveillance systems and tools.
- Management: Review reports and take necessary actions based on findings.

6.Standard Operating Procedures (SOPs) for Surveillance Activities

6.1 Daily Monitoring: SPREAD X review daily transactions for unusual patterns or volumes on above described transaction Analysis rules and pertaining to Surveillance Alert process.

Transaction Activity:

- Frequent Off-Market transfers by a client in a specified period.
- Off-market transfers not commensurate with the income/ Net worth of the client.
- Off-market transfers (High Value) immediately after modification of details in demat account.
- 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.

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

Account Activity:

- Flag accounts exhibiting unusual behaviour for further investigation.
- 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.
- Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
- Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.
- 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.

6.2 Periodic Audits

Quarterly Reviews:

- Conduct comprehensive reviews of participant activities every quarter.
- Document findings and take corrective actions as needed.

Annual Audits:

- Perform a detailed audit of all activities and compliance status annually.
- Ensure adherence to internal policies and regulatory requirements.

6.3 Exception Reporting

Threshold Violations: Report and investigate any transactions exceeding predefined thresholds.
Document the findings and actions taken.

Pattern Recognition:

- Identify and report any irregular trading patterns or suspicious behaviours.
- Utilize data analytics tools for pattern recognition.

6.4 Data Collection and Analysis

Data Sources: Utilize internal systems, regulatory databases, and external reports.
Data Analysis Tools: Employ advanced analytics software to detect anomalies.
Documentation: Maintain detailed records of all analyses and findings.

6.5 Compliance and Reporting

Regulatory Compliance: Ensure all activities comply with relevant regulations (e.g., SEBI guidelines).
Internal Reporting: Generate regular reports for internal review by management and compliance teams.
External Reporting: Submit required reports to regulatory bodies as per mandated schedules.

6.6 Incident Management

Identification: Detect any breaches or suspicious activities.
Investigation: Conduct thorough investigations to understand the root cause.
Resolution: Implement corrective actions and report outcomes to relevant stakeholders.
Follow-Up: Monitor to ensure the issues are resolved and preventive measures are effective.

6.7 Training and Awareness

Regular Training: Provide ongoing training sessions for staff on surveillance techniques and regulatory updates.
Awareness Programs: Conduct awareness programs for depository participants on compliance requirements and best practices.

6.8 Technology and Tools

Surveillance Systems: Use robust systems capable of real-time monitoring and reporting.
Data Security: Ensure data integrity and security through encryption and access controls.

6.9 Review and Improvement

Continuous Improvement: Regularly review and update SOPs to incorporate feedback and adapt to regulatory changes.

6.10 Documentation and Record Keeping

Record Maintenance: Maintain comprehensive records of all surveillance activities for a minimum period as required by regulations.
Documentation Updates: Keep all documentation updated with the latest policies and procedures.

7.Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. All employees are expected to understand and adhere to the guidelines set forth in this policy.

8. Approval and Review

This policy is approved by SPREAD X Management and will be reviewed annually or as required due to regulatory changes or operational needs.