INCRED MARKETS LIMITED
Formerly known as Elite Wealth Limited

DP SURVEILLANCE POLICY AND STANDARD OPERATING PROCEDURE

FOR SURVEILLANCE ALERT GENERATION, REVIEW, INVESTIGATION, ESCALATION AND DISPOSAL

Policy Owner: Compliance Department
Functional Areas: Depository Operations / Compliance / AML
Applicable Depositories: NSDL and CDSL
Effective Date: 01.04.2025
Version: 1.0
Approved By: Board of Directors
Last Reviewed Date-26.07.2026
Review Frequency: At least annually and whenever required by regulatory changes

---

1. PURPOSE

The purpose of this Policy and Standard Operating Procedure ("SOP") is to establish a comprehensive, risk-based and documented surveillance framework for **InCred Markets Limited** ("Company") in its capacity as a Depository Participant of NSDL and CDSL.

The Policy is intended to ensure that the Company:

1. identifies unusual, abnormal or suspicious activities;
2. receives, generates, records and monitors surveillance alerts;
3. conducts appropriate investigation and due diligence;
4. obtains supporting documents and client explanations wherever required;
5. ensures independent review through Maker-Checker controls;
6. escalates material, adverse or suspicious matters;
7. responds to and disposes of depository-generated alerts within the applicable regulatory timeline;
8. makes regulatory/AML reporting wherever required;
9. maintains complete and retrievable records; and
10. periodically reviews the effectiveness of its surveillance mechanism.

The Policy shall be implemented in accordance with applicable SEBI regulations, SEBI Master Circulars, NSDL/CDSL requirements, PMLA requirements and all subsequent circulars, communiqués and directions.

---

2. REGULATORY FRAMEWORK

This Policy shall be read with and subject to the latest applicable provisions of:

2.1 SEBI

a. SEBI Master Circular for Depositories dated December 03, 2024, as amended/supplemented from time to time;

b. Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018, as amended from time to time;

c. applicable SEBI Master Circular on Surveillance of Securities Market;

d. applicable SEBI circulars relating to surveillance, AML/CFT, KYC, risk management and investor protection;

e. any subsequent SEBI circular, notification, direction or clarification applicable to Depository Participants.

SEBI's regulatory database currently records the Depositories Master Circular dated December 03, 2024 and subsequent amendments to the Depositories and Participants Regulations.

2.2 NSDL

a. latest NSDL Master Circular/Operating Instructions for Participants;

b. NSDL surveillance requirements;

c. NSDL surveillance alerts and prescribed response mechanism;

d. NSDL e-PASS requirements;

e. subsequent NSDL circulars/communiqués.

2.3 CDSL

a. latest CDSL Master Circular/Operating Instructions;

b. CDSL surveillance requirements;

c. CDSL surveillance alerts;

d. CDSL prescribed response/disposal mechanism;

e. subsequent CDSL communiqués/circulars.

2.4 AML/PMLA

a. Prevention of Money Laundering Act, 2002;

b. Prevention of Money-laundering (Maintenance of Records) Rules;

c. applicable FIU-IND requirements;

d. applicable SEBI AML/CFT requirements.

2.5 Other Regulatory Requirements

Where applicable, the Company shall also comply with surveillance requirements issued by:

- NSE;
- BSE;
- MCX;
- NCDEX; and
- any other recognised Stock Exchange or regulatory authority with which the Company is registered.

In case of any inconsistency between this SOP and a subsequent regulatory circular/communiqué, the applicable regulatory requirement shall prevail and this SOP shall be amended accordingly.

---

3. POLICY STATEMENT

InCred Markets Limited shall maintain an effective surveillance mechanism proportionate to:

- nature and size of its business;
- number of Beneficial Owner accounts;
- transaction volumes;
- client profile;
- risk classification;
- nature of securities handled;
- off-market transaction activity;
- pledge/release activity;
- account modifications;
- dormant/inactive accounts;
- regulatory alerts; and
- other identified risk factors.

The Company shall maintain surveillance arrangements covering both:

A. Depository-generated alerts

Alerts received from NSDL/CDSL.

B. DP-generated alerts

Alerts generated internally by InCred Markets Limited based on its own risk assessment, client profile and transaction activity.

The Company shall not restrict its surveillance mechanism only to alerts received from the Depositories.

---

4. GOVERNANCE AND RESPONSIBILITY

4.1 Board of Directors

The Board shall:

1. approve the Surveillance Policy;
2. ensure appropriate governance over the surveillance framework;
3. ensure availability of adequate systems, personnel and resources;
4. review material surveillance/compliance issues, where required;
5. ensure appropriate corrective action for material deficiencies; and
6. review the Policy periodically.

4.2 Compliance Officer

The Compliance Officer shall have overall supervisory responsibility for implementation of the surveillance framework and shall:

1. ensure implementation of this Policy;
2. monitor regulatory alerts and ageing;
3. review material/adverse cases;
4. ensure timely responses to NSDL/CDSL;
5. ensure escalation of suspicious matters;
6. coordinate with the Principal Officer for AML/PMLA matters;
7. monitor regulatory reporting;
8. ensure maintenance of surveillance records;
9. review repeat/adverse alerts; and
10. ensure periodic review and updating of surveillance parameters.

4.3 Principal Officer

The Principal Officer shall examine cases requiring AML/PMLA consideration and shall take appropriate action, including STR reporting to FIU-IND wherever required.

4.4 Maker

The Maker shall:

- download/identify alerts;
- conduct preliminary and detailed review;
- analyse client and transaction information;
- obtain explanations/documents;
- document findings;
- prepare the investigation report; and
- recommend closure, monitoring or escalation.

4.5 Checker

The Checker shall independently review:

- investigation;
- client profile;
- transaction details;
- supporting documents;
- client explanation;
- findings;
- classification;
- proposed action; and
- proposed regulatory reporting.

The Checker shall not merely rely on the Maker's conclusion without reviewing the underlying evidence.

---

5. SURVEILLANCE ALERT SOURCES

Surveillance alerts may arise from:

1. NSDL;
2. CDSL;
3. internal surveillance systems;
4. Stock Exchanges;
5. AML/KYC monitoring;
6. internal audit;

7. concurrent audit;
8. client complaints;
9. regulatory communications;
10. transaction monitoring;
11. employee escalation;
12. law-enforcement/regulatory communication; and
13. any other reliable source.

---

6. INTERNAL SURVEILLANCE FRAMEWORK

InCred Markets Limited shall establish and maintain internal surveillance parameters based on the risk profile of its DP business.

The parameters shall be reviewed periodically and modified whenever required due to:

- regulatory changes;
- changes in business profile;
- emerging risks;
- inspection observations;
- repeated alerts;
- suspicious transaction trends;
- changes in transaction volumes; or
- instructions issued by NSDL/CDSL/SEBI.

The surveillance framework shall include suitable preventive/detective controls and an appropriate audit trail.

---

7. MINIMUM SURVEILLANCE PARAMETERS

The following shall be considered as part of the Company's surveillance framework, wherever relevant.

7.1 High-Value Transactions

Transactions substantially higher than the client's known profile, financial capacity or normal activity.

7.2 Off-Market Transfers

Monitoring of:

- high-value off-market transfers;
- frequent off-market transfers;
- transfers between unrelated accounts;
- unusual transfer patterns;
- transfers inconsistent with client profile;

- repeated transfers involving common accounts.

7.3 Multiple Accounts/Common Attributes

Monitoring of accounts having common:

- PAN;
- mobile number;
- email ID;
- address;
- bank account;
- other relevant demographic attributes.

7.4 Account Modifications

Monitoring of:

- frequent address changes;
- frequent mobile/email changes;
- bank-account modifications;
- authorised-signatory changes;
- changes followed by significant transactions;
- other unusual modifications.

7.5 Dormant/Inactive Accounts

Monitoring of:

- sudden activation;
- high-value transactions following activation;
- substantial securities movement;
- unusual activity after prolonged inactivity.

7.6 Pledge/Release

Monitoring of:

- unusual/high-value pledges;
- frequent pledge/release;
- pledge activity inconsistent with client profile;
- unusual securities movement around pledge transactions.

7.7 Dematerialisation/Rematerialisation

Monitoring of unusual or abnormal demat/remat activity inconsistent with the client's profile.

7.8 Other Activity

The Company shall also monitor any other activity prescribed by SEBI, NSDL, CDSL or Stock Exchanges.

---

8. ALERT REGISTERING

Every surveillance alert shall be assigned a unique reference number.

The Surveillance Alert Register shall capture at least:

- Alert ID;
- source;
- date of generation/receipt;
- Depository;
- DP ID;
- BO ID;
- PAN;
- alert category;
- transaction details;
- transaction value;
- prescribed response date;
- Maker;
- Checker;
- current status;
- ageing; and
- date of disposal/reporting.

---

9. PRELIMINARY REVIEW

The Maker shall review the alert against:

1. client KYC;
2. client occupation/business;
3. income/net worth;
4. risk classification;
5. account opening information;
6. bank details;
7. securities holdings;
8. transaction history;
9. previous alerts;
10. related/common accounts;

11. transaction counterparties;
12. nature and purpose of transaction; and
13. any other relevant information.

---

10. ENHANCED REVIEW

Where the alert cannot be satisfactorily explained from existing records, the Company shall undertake enhanced review.

This may include obtaining:

- client written explanation;
- bank statement;
- demat statement;
- source of funds/securities;
- transaction agreement;
- invoice;
- gift deed;
- loan documentation;
- relationship proof;
- financial statements;
- income/net-worth evidence;
- corporate documents; or
- other relevant evidence.

The level of investigation shall be proportionate to the risk.

---

11. CLIENT COMMUNICATION

Where clarification is required, the Company may communicate with the client through approved communication channels.

The communication shall:

- clearly identify the information required;
- avoid disclosure of confidential regulatory information;
- prescribe a reasonable response period;
- maintain evidence of communication; and
- be preserved with the alert record.

Nothing in this section shall require the Company to disclose an STR or information where such disclosure is prohibited by applicable law.

---

12. INVESTIGATION DOCUMENTATION

For each alert, the Maker shall record:

1. reason for alert;
2. transaction details;
3. client profile;
4. review conducted;
5. documents examined;
6. client explanation;
7. relationship between parties, where relevant;
8. comparison with normal activity;
9. previous similar activity;
10. adverse indicators, if any;
11. conclusion; and
12. proposed action.

The investigation shall be sufficiently detailed to enable an independent reviewer, auditor, Depository or regulator to understand the basis of the decision.

---

13. ALERT CLASSIFICATION

Following investigation, the alert shall be classified as:

Category A – Verified and Closed

The transaction/activity has been satisfactorily explained and no adverse observation remains.

Category B – Verified and Kept Under Monitoring

The activity is explainable but requires enhanced/continued monitoring.

Category C – Adverse / Escalated

The explanation/documents are unsatisfactory or the activity remains unusual/suspicious.

Category D – Reported

The matter has been reported to the concerned Depository, Stock Exchange, SEBI, FIU-IND or other competent authority, as applicable.

---

14. DISPOSAL OF NSDL ALERTS

NSDL alerts shall be investigated and responded to through the prescribed NSDL mechanism.

The response shall be supported by the underlying investigation and documentary evidence.

The Company shall comply with the **currently applicable NSDL response timeline**.

NSDL revised the surveillance-alert response timeline from 30 days to **45 days with effect from April 1, 2025**. The applicable NSDL circular/communication and any subsequent amendment shall be followed.

The Company shall not wait until the last day for disposal and shall maintain internal ageing controls to ensure timely response.

---

15. DISPOSAL OF CDSL ALERTS

CDSL alerts shall be:

1. recorded;
2. investigated;
3. appropriately classified;
4. supported with relevant records;
5. reviewed by the Checker; and
6. responded to/disposed through the prescribed CDSL mechanism.

The **timeline specifically applicable to the particular CDSL alert category shall be followed**.

The standard surveillance-alert timeline and any category-specific extension prescribed by CDSL shall be monitored separately.

For example, CDSL has subsequently prescribed a **60-day period for the specified alert category for which the period was extended from 45 days to 60 days**.

Accordingly, the Company shall maintain an alert-wise "Regulatory Due Date" rather than applying a blanket timeline to every alert.

---

16. REGULATORY DUE-DATE CONTROL

For every depository alert, the system/register shall capture:

Alert Date + Applicable Regulatory Timeline = Regulatory Due Date

The Compliance Department shall verify the applicable timeline based on:

- Depository;
- alert type;
- date of generation;
- applicable circular/communiqué; and
- any subsequent amendment.

The latest applicable Depository instruction shall prevail.

---

17. INTERNAL AGEING CONTROL

The Company shall use the following internal escalation mechanism:

Ageing	Internal Control
0–15 days	Investigation
16–30 days	Investigation/Checker review
31 days onwards	Compliance monitoring
5 working days before regulatory due date	Mandatory Compliance escalation
2 working days before regulatory due date	Senior escalation
Regulatory due date	Response/disposal must be completed

These are **internal control timelines** and shall not replace or override the regulatory timeline.

Where the regulatory timeline is shorter, the shorter regulatory timeline shall prevail.

---

18. OVERDUE ALERTS

Any alert approaching or exceeding its regulatory due date shall be immediately escalated to the Compliance Officer.

Where an alert becomes overdue:

1. reason for delay shall be recorded;
2. root cause shall be identified;
3. corrective action shall be documented;
4. management shall be informed where material;
5. regulatory response shall be submitted immediately;
6. applicable Depository penalty/disciplinary consequences shall be reviewed; and
7. recurrence-prevention measures shall be implemented.

---

19. ADVERSE/SUSPICIOUS ACTIVITY

An alert shall be treated as adverse/suspicious where, based on available information:

- transaction rationale is not satisfactory;
- supporting documents are inadequate;
- activity is inconsistent with the client profile;
- activity indicates possible layering/structuring;
- multiple accounts appear connected;
- securities are moved without apparent economic rationale;
- unusual activity continues despite clarification;
- information appears false/inconsistent; or
- any other material red flag exists.

Such matters shall be escalated to the Compliance Officer and, where applicable, Principal Officer.

---

20. AML/PMLA ESCALATION

Where the facts indicate possible money laundering, terrorist financing or other suspicious activity covered under applicable AML/PMLA requirements, the matter shall be referred to the Principal Officer.

The Principal Officer shall determine appropriate action, including STR filing with FIU-IND where required.

The surveillance process shall operate independently of the STR decision-making process, while ensuring appropriate escalation and confidentiality.

No employee shall disclose the filing or proposed filing of an STR where such disclosure is prohibited.

---

21. REGULATORY REPORTING

Depending on the facts and applicable regulatory requirements, the Company shall report to:

- NSDL;
- CDSL;
- NSE;
- BSE;
- MCX;
- NCDEX;
- SEBI;
- FIU-IND; or

- other competent authority.

All regulatory submissions shall be made within the applicable prescribed timeline.

Evidence of submission shall be retained.

---

22. MAKER-CHECKER

No surveillance alert shall be considered finally disposed of solely on the basis of the Maker's review where Maker-Checker review is applicable.

The Checker shall independently verify:

- alert;
- transaction;
- client profile;
- investigation;
- documents;
- client explanation;
- conclusion;
- classification; and
- regulatory reporting requirement.

Material/adverse cases shall be reviewed by the Compliance Officer.

---

23. SURVEILLANCE ALERT REGISTER

The Company shall maintain a central register containing, at minimum:

Particular	Requirement
Alert ID	Mandatory
Source	NSDL/CDSL/Internal/Exchange
Alert Date	Mandatory
Regulatory Due Date	Mandatory
DP ID	Mandatory
BO ID	Mandatory
PAN	Mandatory
Alert Parameter	Mandatory
Transaction Date	Where applicable
Transaction Value	Where applicable
Client Profile	Review
Documents	Details
Client Explanation	Details

Maker Finding	Mandatory
Checker Finding	Mandatory
Compliance Finding	Where applicable
Classification	Mandatory
Action Taken	Mandatory
Regulatory Reporting	Where applicable
Date of Response	Mandatory
Date of Closure	Mandatory
Delay	Yes/No
Reason for Delay	If applicable
Supporting Evidence	Mandatory

---

24. EVIDENCE AND AUDIT TRAIL

For every alert, the Company shall maintain an audit trail sufficient to establish:

Alert → Investigation → Evidence → Client Explanation → Maker Finding → Checker Review → Compliance Decision → Regulatory Response → Closure

Electronic records shall preserve, wherever feasible:

- date/time;
- user ID;
- action performed;
- modification history;
- approval;
- closure date; and
- regulatory submission evidence.

---

25. RECORD RETENTION

All surveillance records shall be retained for the period prescribed under the applicable:

- SEBI regulations;
- Depository requirements;
- PMLA requirements;
- Exchange requirements; and
- other applicable laws/regulations.

Where more than one retention period applies, the **longer applicable retention requirement shall be followed**.

Records shall be readily retrievable for inspection by SEBI, NSDL, CDSL, Stock Exchanges, auditors or other authorised authorities.

26. CONFIDENTIALITY

Surveillance investigations shall be treated as confidential.

Access shall be restricted to authorised personnel on a need-to-know basis.

Information relating to:

- surveillance investigations;
- suspicious activity;
- STR consideration;
- regulatory investigations; and
- regulatory correspondence

shall not be disclosed except as permitted/required under applicable law.

---

27. SYSTEM AND ACCESS CONTROL

Access to surveillance systems/registers shall be role-based.

The Company shall maintain appropriate controls over:

- user access;
- data modification;
- alert closure;
- approval;
- deletion;
- audit trail; and
- regulatory submission.

User access shall be reviewed periodically and immediately upon change in employee role or cessation of employment.

---

28. BUSINESS CONTINUITY

The Company shall maintain appropriate backup arrangements for surveillance records and regulatory submissions.

In the event of system failure, the Compliance/DP Operations team shall use an approved alternate/manual process to ensure that regulatory timelines are not missed.

All manually processed alerts shall subsequently be updated in the designated system/register.

29. PERIODIC REVIEW

The Compliance Department shall periodically review:

1. pending alerts;
2. ageing;
3. overdue alerts;
4. repeat alerts;
5. adverse alerts;
6. regulatory reporting;
7. quality of investigation;
8. quality of closure remarks;
9. alert parameters;
10. system effectiveness;
11. false positives;
12. inspection observations; and
13. corrective actions.

30. SURVEILLANCE PARAMETER REVIEW

Surveillance parameters shall be reviewed at least annually and additionally whenever required.

The review shall consider:

- regulatory changes;
- Depository circulars;
- new alert themes;
- changes in client behaviour;
- transaction volumes;
- historical suspicious activity;
- audit/inspection findings;
- system capabilities; and
- emerging market risks.

Any material change shall be approved by the competent authority.

31. INTERNAL AUDIT / CONCURRENT AUDIT

The surveillance mechanism shall be subject to appropriate independent review through internal/concurrent/statutory audit, as applicable.

The review shall specifically verify:

- completeness of alerts;
- timely investigation;
- regulatory due dates;
- quality of disposal;
- supporting documentation;
- Maker-Checker control;
- escalation;
- regulatory reporting;
- overdue alerts; and
- audit trail.

Exceptions shall be documented and corrective action monitored to closure.

---

32. MANAGEMENT INFORMATION SYSTEM (MIS)

The Compliance Department shall maintain periodic MIS covering:

- total alerts;
- NSDL alerts;
- CDSL alerts;
- internal alerts;
- closed alerts;
- monitored alerts;
- reported alerts;
- pending alerts;
- overdue alerts;
- alerts nearing due date;
- repeat alerts;
- adverse alerts; and
- regulatory penalties, if any.

Material exceptions shall be escalated to Senior Management/Board as appropriate.

---

33. TRAINING

Employees involved in:

- Depository Operations;
- Compliance;
- AML/KYC;
- Surveillance;
- Risk Management; and
- Customer Service

shall receive appropriate training regarding:

- surveillance requirements;
- alert investigation;
- red flags;
- documentation;
- escalation;
- confidentiality;
- PMLA/AML requirements; and
- regulatory timelines.

Training records shall be maintained.

---

34. NON-COMPLIANCE

Failure to:

- identify;
- investigate;
- document;
- escalate;
- respond to; or
- dispose of

surveillance alerts within the applicable regulatory requirements shall be treated as a compliance exception.

Material/repeated exceptions shall be escalated to Senior Management and the Compliance Officer.

Root-cause analysis and corrective/preventive action shall be undertaken.

---

35. REGULATORY CHANGE MANAGEMENT

The Compliance Department shall monitor circulars/communications issued by:

- SEBI;
- NSDL;
- CDSL;
- NSE;
- BSE;
- MCX;
- NCDEX;
- FIU-IND; and
- other applicable authorities.

Any regulatory change affecting surveillance shall be:

1. identified;
2. assessed;
3. mapped to this Policy/SOP;
4. incorporated into operating procedures;
5. communicated to relevant employees; and
6. implemented within the prescribed effective date.

---

36. POLICY REVIEW

This Policy shall be reviewed:

- at least annually;
- upon any material regulatory change;
- upon any significant surveillance incident;
- upon material audit/inspection observation;
- upon introduction of new products/services; or
- whenever otherwise considered necessary by Compliance.

The latest applicable regulatory requirement shall prevail over any inconsistent provision in this Policy.

---

37. EFFECTIVE DATE AND APPROVAL

This Policy shall come into effect from 01.04.2025 and shall remain effective until amended or replaced.

For InCred Markets Limited
Formerly known as Elite Wealth Limited
