CDSL/AUDIT/DP/POLCY/2026/151 **March 05, 2026**

SOP FOR HANDLING CYBER INCIDENT AND AMENDMENTS TO DP OPERATING INSTRUCTIONS ANNEXURE 11.1

Depository Participants (DPs) are advised to take note Standard Operating Procedure (SOP) for handling the Cyber incident and accordingly amendments in CDSL's DP Operating Instructions Annexure 11.1 – Penalty Structure for DPs for handling Cyber Security incidents has been updated in co-ordination with other Depositories and Exchanges.

RE/ Depository Participants (DP)/ Member shall ensure to report any cyber security incident within 6 hours of noticing /detecting such incident or being brought to the notice about such incidents (In case of inability in submitting cyber security incident by REs/ Depository Participants (DP)/Member may report the cyber incident over email in the prescribed format on common group email ID specified by SEBI/Market Infrastructure Institutions (MIIs) , so as to ensure adherence with the above prescribed timelines of 6 hours). Further, the Depositories / Exchanges may take /implement various precautionary containment measures /action to prevent any lateral movement of the threat /malware to the Depositories/ Exchanges or to other Trading Member networks through Depository / Exchange connectivity. The following precautionary measures /action may be taken based on the classification /severity of the reported cyber incident.

DPs are advised to take note of the afore-mentioned amendments to the Operating Instructions. Annexure 11.1. Please refer Annexure A for Standard Operating Procedure (SOP) **for handling the Cyber incident.**

Queries regarding this communiqué may be addressed to CDSL by emails to: dpinfosec@cdslindia.com and connect through our IVR Number 022-62343333.

For and on behalf of
Central Depository Services (India) Limited

sd/-

Mrugen Vijay Munjpara
Assistant Vice President – Information Security

Internal

Annexure I

In case of non-submission of Cyber incident, Mitigation Report, RCA, VAPT Report & Forensic Audit Report Penalty as stated are not submitted within the timelines, following penalties shall be applicable to such DPs:-

Table-3

Sr. No.	Nature of non-compliance		Penal Action (in Rs.)	
	Penalty for not submitting the above reports within due date	**Timeline**	**For All Members/ DPs (other than QSB/QREs)**	**For QSB/QRE Members**
1	Non-submission of Cyber Incident reporting (Immediate Submission) within the time specified by the Exchange and Depository.	Within 6 hours	If the incident is not reported within 6 hours. Rs. 20,000/- per day till the incident is reported subject to a maximum of Rs. 2 lakhs per incident.	If the incident is not reported within 6 hours. Rs. 20,000/- per day till the incident is reported subject to a maximum of Rs. 10 lakhs per incident.
2	Submission of Mitigation Report, Root Cause Analysis Report, Forensic Audit Report & VAPT Report	Within 07 calendar Days from the Due Date till submission whichever is earlier	Rs. 1500 per day	Rs. 3000 per day
		From 08th to 21st calendar day from the Due Date till submission whichever is earlier.	Rs. 2500 per day	Rs. 5,000 per day
		From 22nd calendar day from due date till submission	New Account Opening to be restraint. The notice of New Account Opening Restraint issued to the member/ DP will be shared with all the MII's for information.	

Internal

Sr. No.	Nature of non-compliance		Penal Action (in Rs.)	
	Penalty for not submitting the above reports within due date	Timeline	For All Members/ DPs (other than QSB/QREs)	For QSB/QRE Members
3	In case press release is not issued within a one working day from the intimation of normalcy of operation to Depositories /Exchange(s)/. (QRE/QSB)		Penalty of Rs. 50,000- in case PR is issued post one working day and thereafter penalty of Rs 10,000/- per working day for any additional delay subject to maximum penalty of Rs 1,00,000/-.	

Note: For the reported cyber incident, the applicable penalty (if any) as mentioned in Table- 3 above, shall be levied by any one Exchange /Depository to whom said incident has been assigned for handling as per this SOP

Table- 4

Penalty which shall be applicable based on review of Member/DP submissions by the Joint/ Relevant Committee of Exchange(s)/Depositories:-

In case the report (as stated under Table 1) are found to be inaccurate or incomplete /missing component in any manner (for instance-no identification or incorrect identification of root cause ,inaccurate sequence of events, missing /incomplete component etc and if the cyber incident occurred on account of noncompliance of SEBI cyber security policies and guidelines ,penalties as prescribed under shall be applicable to such DPs/Members.

Sr. No	Nature of non-compliance	Penal Action (in Rs.)	
	Particulars	For All Members/ DPs (other than QSB/QREs)	For QSB/QRE Members
1	In case the above-mentioned Report / Activity are found to be deficient or incomplete / missing component in any manner by the Joint / Relevant Committee of Exchange(s)/ Depositories	Rs 50,000/- per incomplete/missing component	Rs 1,00,000/- per incomplete/missing component
2	In case the report is found to be misleading or inaccurate	Rs 1,00,000/- per misleading or	Rs 2,00,000/- per misleading or

Internal

Sr. No	Nature of non-compliance	Penal Action (in Rs.)	
	Particulars	For All Members/ DPs (other than QSB/QREs)	For QSB/QRE Members
		inaccurate component	inaccurate component
3	In the event of the REs not submitting accurate and complete reports after being provided additional time (if provided by the Joint / Relevant Committee of Exchange(s)/ Depositories)	Rs 2,00,000/-	Rs 4,00,000/-
4	If the Joint / Relevant Committee of Exchange(s)/ Depositories determines that the incident occurred on account of non-compliance of SEBI cyber security policies and guidelines such as incident happened due to a vulnerability existing in the system and the vulnerability was not identified during VAPT prior to incident and/or incident happened due to a vulnerability was not closed and incident happened outside the VAPT closure timelines.	Rs 2,00,000/- per non-compliance	Rs 4,00,000/- per non-compliance

Note: For the reported cyber incident, the applicable penalty (if any) as mentioned in Table- 4 above, shall be levied by any one Exchange /Depository to whom said incident has been assigned for handling as per this SOP.

Internal

Table 5

In case recommendations of Joint /Relevant Committee of Depositories / Exchange(s) are not implemented by them within prescribed timeline, the following progressive slab-wise structure for imposition of "Penalty /Regulatory Action" shall be followed from the expiry of the deadline specified by Joint. Relevant Committee of Depositories /Exchanges(s):-

Sr. No	Nature of non-compliance	Penal Action (in Rs.)	
	Penalty in case of delay beyond the deadline as specified by Joint / Relevant Committee of MIIs/Exchange(s)/Depositories for Non-Implementation / Non-submission of confirmation	**For All Members/ DPs (other than QSB/QREs)**	**For QSB/QRE Members**
1	Charges per day for the first 7 calendar days or till submission of report from the prescribed deadline, whichever is earlier.	Rs. 10,000 per day	Rs. 20,000 per day
2	Charges per day from 8th calendar day to 21st calendar day or submission of report from the prescribed deadline, whichever is earlier.	Rs. 20,000 per day	Rs. 40,000 per day
3	In case of non-submission / non implementation of recommendations of Joint/ Relevant Committee of Exchange(s)/ Depositories within 21 calendar day from the prescribed deadline of submission	New Account Opening to be restraint. The notice of New Account Opening Restraint issued to the member will be shared with all the Exchanges / Depositories for information.	

Note: For the reported cyber incident, the applicable penalty (if any) as mentioned in Table- 5 above, shall be levied by any one Exchange /Depository to whom said incident has been assigned for handling as per this SOP.

Internal

SOP for Inter-MII to handle Cyber incident

Central Depository Services (India) Limited

CDSL

Convenient • Dependable • Secure

SOP for Inter-MII to handle Cyber incident

Version 1.0

9 May 2025

CDSL

REVISION CONTROL

Revision	Revision Date	Type of Changes	Author	Reviewed By	Approved By
1.0	9 May 2025	Initial Document	Information Security Implementation Team (ISIT)	Mrugen Munjpara	Akhil Wadhavkar

Internal

CDSL

Table of Contents

Internal

CDSL

1. Objective of the SOP

- Provide step-by-step instruction for the Inter-MII Committee towards performing activities & tasks related to Cyber Incident reported by the Trading Members / DP.
- To outline the actionable defined by the SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, regarding Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).
- Ensure a standardized basis for communication & coordination in the Inter-MII committee.
- To ensure Consistency, Quality, Compliance, & Enforcement in related processes.

2. Scope of the SOP

- Registered members of all Exchange and Depository,
- Exchange and Depository (NSE, BSE, MCX, NCDEX, MSEI, NSDL, CDSL),
- And all people, processes and technology are required to support the objectives.

3. Constitution of the Committee

- A joint Inter-MII committee will be constituted comprising of representatives from Information Security, IT, legal & Compliance, Member Compliance, at least 2 representatives from each Exchange and Depository.
- The constitution of the committee shall be reviewed annually at the end of the financial year. Ad hoc inclusion/removal may be initiated on request of the Exchange and Depository.
- Current Committee Members –

CDSL

Table 1			
Name of Member	**Exchange & Depository**	**Email ID**	**Contact details**
Mr. Devendra Kulkarni	BSE	devendra.kulkarni@bseindia.com	+91- 9820732466
Mr. Maharshi Mekhia	BSE	maharshi.mekhia@bseindia.com	+91- 8425954567
Mr. Sateesh Kaka	BSE	sateesh.kaka@bsetech.in	+91- 8404988748
Mr. Abhijeet Sontakke	NSE	asontakke@nse.co.in	+91- 9820108756
Mr. Prashant Aier	NSE	paier@nse.co.in	+91- 9819067608
Mr. Mukesh Addagatla	NSE	maddagatla@nse.co.in	+91- 8655647625
Mr. Gunjesh Rai	MCX	gunjesh.rai@mcxindia.com	+91- 8356842457
Mr. Denny Paul	MCX	denny.paul@mcxindia.com	+91- 9987587710
Mr. Krunal Rahangadale	MCX	krunal.rahangadale@mcxindia.com	+91- 8433911822
Ms. Archana Venugopal	NCDEX	archana.venugopal@ncdex.com	+91- 8113011166
Mr. Shantaling Houde	NCDEX	shantaling.houde@ncdex.com	022-66406507
Mr. LaxmiNarayan Sahu	MSEI	LaxmiNarayan.Sahu@msei.in	+91- 9776018333
Mr. Hasan Ambalge	MSEI	hasan.ambalge@msei.in	+91- 9821648904
Mr. Soleha Sayyed	MSEI	soleha.sayyed@msei.in	+91- 8433583088
Ms. Aarti Chitnis	CDSL	aartic@cdslindia.com	022-6234 3576
Mr. Ankur Chatterjee	CDSL	ankurc@cdslindia.com	022-6234 3281
Mr. Mrugen Munjpara	CDSL	mrugenm@cdslindia.com	+91- 9136565108
Ms. Nikita Joshi	NSDL	dpinfosec@nsdl.com	+91- 8655238446
Mr. Dheeraj Singh	NSDL	Dheeraj.Singh@nsdl.com	+91- 9619030390

3.1 **Roles and Responsibilities of the Committee**

- The Committee shall propose a way to Allocate or distribute Common Trading Member equally between all Exchange and Depository. Exclusive members registered with the Exchange and Depository would continue to be responsibility of the registered Exchange and Depository for the entire Cyber Security domain.

- All reporting cases shall be allocated sequentially among the Exchange and Depository by the joint Inter-MII committee. Each reporting case will be handled by one Lead Exchange and One Lead Depositories.
- Further, the Member associated only with the specific Exchange and Depository, an independent review/assessment of such incidents will be done by that respective Exchange and Depository.
- The reporting may be presented to the committee by the respective Exchange and Depository for any recommendation.
- The Committee shall develop and review guidelines (yearly) w.r.t Cyber Incidents Root Cause Analysis (RCA) reports along with recommendations from, and Financial Disincentives prescribed as per the Framework to address the 'Cyber Incidents' in Stockbrokers' Electronic Trading Systems and recommendations of SEBI.

3.2 **Periodicity of Committee Meetings**

- The committee can meet at least once a month, preferably in the last week of the month, wherein the respective Exchange and Depository can present their allotted cases with recommendations if any.
- The committee, based on the analysis, shall deliberate and advise on the necessary measures, including taking any disciplinary action.
- The committee meeting shall be organized by the Exchange and Depository on a rotational basis. The assigned Exchange and Depository shall be responsible for scheduling the meeting, drafting the agenda, and preparing/circulating the minutes of the meeting. The minutes of the meeting will also be circulated to SEBI whenever required.

4. Trading Member Compliance Requirements

4.1 **Reporting:**

- All Members shall report the Cyber Incident through earmarked Email-Id ("member.cir@bseindia.com") as mentioned in the reporting structure of the Framework.
- Members are required to provide essential details while reporting an incident to facilitate effective investigation
- Guidelines w.r.t reporting within timelines shall be adhered to by member stockbrokers of all Exchange and Depository.

4.2 **Timelines:**

- The timelines applicable for following post incident reporting(s) / submissions by the REs/Trading Members/DP to SEBI/Exchange/Depository shall be as under Table 2:

Table 2		
Sr. No.	**Name of the Report / Activity**	**Timeline for Submission**
1	Submission of Cyber Incident reporting (Immediate Submission)	Within 6 hours
2	Immediate Mitigation Measure Report	On same day
3	Press Release	T#+1 Day
4	Interim Report*	T#+3 Days
5	Mitigation Measure Report**	T#+7 Days
6	Root Cause Analysis (RCA)*** report along with recommendations from Technology Committee of the RE	T#+30 Days##
7	Forensic Audit Report (on the incident) and its closure report****	Refer clause Forensic Investigation/ Audit given below****
8	Vulnerability Assessment and Penetration Testing (VAPT) for cyber incident and its closure reports	T#+45 days
9	Any other report advised by Exchange/Depository/SEBI	To be submitted as per timelines advised by Exchange/Depository/SEBI

T day refers to day of noticing / detecting such incidents or being brought to notice about such incidents.

Additional time may be granted by SEBI/ MIIs for the submission of RCA on a case-by-case basis on request of the RE taking into account the complexity and nature of the incident(s). The same shall be an exception rather than the rule.

*The interim report must contain, inter alia, the following: Details of the incident including time of occurrence, information regarding affected processes/ systems/ network/ services, severity of the incident, measure taken to contain and the steps taken to initiate the process of response and recovery.

** Mitigation Measure Report to describe immediate action taken by the Trading Members/DP upon noticing / detecting such incidents or being brought to the notice about such incidents.

***The RCA report should inter-alia include exact cause of the incident (including root cause from vendor(s), if applicable), exact timeline and chronology of the incident, details of impacted processes/ systems /network /services, details of corrective/ preventive measures taken (or to be taken) by the entity along with timelines and any other aspect relevant to the incident. RCA should be mapped with 'Cyber Kill Chain' framework.

Additionally, it should also include time when operations/ functions/ services were restored and in the event of a disaster, time when disaster was declared. If a similar

incident is repeated, then the status of measures identified previously should be listed and any discrepancies are to be highlighted.

****Forensic Investigation/ Audit

- For all incidents classified as High or Critical, the Trading Members/DP shall submit a forensic audit/ investigation report.
- For incidents classified as low or medium, forensic reports shall be submitted if the RCA is inconclusive or if the SEBI/ Exchange and Depository directs the same.
- After the completion of forensic audit, Trading Members/DP shall submit a final closure report, which shall include the root cause of the incident, its impact and measures to prevent recurrence. The timeline for submission of the reports (including closure reports), shall be decided based on discussion with all stakeholders. However, the maximum period for the submission of forensic audit report shall be 75 days from the date of reporting of incident. In case the report is not submitted by the RE within the prescribed timeline, an appropriate regulatory action may be taken.
- For all the issues/ observations submitted in the forensic report, the Trading Members/DP shall provide a timeline for fixing the same. This timeline shall be submitted along with the forensic investigation/ audit report. Once the issues are resolved, the Trading Members/DP shall file a closure report for the same after review (of the report) by respective IT Committee for Trading Members/DP.
- In case the issues are not fixed within the prescribed timeline, appropriate regulatory action may be taken as deemed fit depending on the nature of the incident.

5. Procedures

5.1 Communication with stakeholders

- All the reported Incident would be analyzed by allotted Exchange and Depository and may be discussed by the Inter-MII Committee in a periodic meeting/ad hoc meeting based on criticality.
- In addition to the above, considering the
  - Criticality of the cyber security incident (viz; Critical / High / Medium).
  - Number of active clients with the said Trading Member/RE (viz; equal to or greater than 50,000 active UCC clients as on March 31).
  - Registered with Depositories as Institutional or Non- Institutional DP.
  - And any other parameters as defined from time to time, the matter may be placed before the Joint / Relevant Committee of the Exchange and Depository(s)/Depositories.

- Email Communication and Ad hoc Meetings may be conducted with Members for clarifications on the compliance requirements of the Framework on Cyber Incidents
- The Committee may communicate with the Regulator.

5.2 **Maintenance of MIS & Incident Handling on Cyber Incident**

- MIS is to be maintained for all the Cyber incidents reported by the Trading Members/DP. The said MIS shall include all relevant details of the cyber-Incident as mentioned in Annexure C of SEBI CSCRF dated 20th August 2024. The MIS is required to be shared with the Exchange and Depositorys till the 5th day of the subsequent month.
- During the life cycle of incident handling, the following aspects need to be broadly covered/captured:
    - Whether the Trading Members/DP has followed the incident response plan of their organization while handling the incident.
    - Whether the Trading Members/DP has taken necessary (immediate) measures to contain the incident impact.
    - Whether the Trading Members/DP has communicated to all relevant stakeholders about the incident.
    - Whether Trading Members/DP has taken sufficient measures to control, mitigate and remediate the incident.
    - Whether Root cause analysis (RCA) has been performed by Trading Members/DP.
    - Whether lessons learnt have been implemented by Trading Members/DP.
    - Whether the issues/loopholes identified in RCA stage have been addressed/plugged by the Trading Members/DP.
    - Whether Trading Members/DP has hired any CERT-In Emplaned independent agency to conduct IS Audit/ forensic audit related to the incident (as per applicability).
    - Whether Trading Members/DP has addressed/plugged vulnerabilities identified in the audit mentioned in point above.

6. Enforcement/ Financial Disincentive

- As the reporting of cyber incident is uniform across all the Exchange and Depository, For critical/high category incidents with possibility of lateral spread, the connectivity between the Trading Member/DP and Exchanges/Depositories– COLO/POP/SFTP/API, shall be kept disabled.
- The connectivity shall be restored, ONLY once the Trading Member/DP submits “Immediate Mitigation Measure Report, certified by a Cert-In empaneled Auditor

which shall certify that, "the Risk with respect to the reported Cyber security Incident has been completely mitigated and there is NO potential for any lateral movement of the threat/malware to the Exchange/Depository or to other Trading Member/DP networks through Exchange/Depository connectivity of the Trading Member/DP."

- In case, Non-submission of Cyber Incident, Mitigation Report, RCA, Forensic Audit Report, VAPT Report as stated under Table 2 are not submitted within the timelines, following penalties shall be applicable to such Trading Members / RE / DP:

  Please refer the Table 3 of the Annexure I.

- In case the reports (as stated under Table 2) are found to be inaccurate or incomplete / missing component in any manner (for instance - no identification or incorrect identification of root cause, inaccurate sequence of events, missing / incomplete component, etc.) and if the cyber incident occurred on account of non-compliance of SEBI cyber security policies and guidelines, penalties as prescribed under Table 4 below shall be applicable to such Trading Members/ DPs:

  Please refer the Table 4 of the Annexure I.

Note- For the reported cyber incident, the applicable penalty (if any) as mentioned in Table-4 above, shall be levied by any one Exchange /Depository to whom said incident has been assigned for handling as per this SOP.

- In case recommendations of Joint / Relevant Committee of Exchange(s)/Depositories are not implemented by them within the prescribed timeline, the following progressive slab-wise structure for imposition of "Penalty / Regulatory Action" prescribed under Table 5 shall be followed from the expiry of the deadline specified by Joint / Relevant Committee of Exchange(s)/Depositories: -

  Please refer the Table 4 of the Annexure I

Note: For the reported cyber incident, the applicable penalty (if any) as mentioned in Table-5 above, shall be levied by any one Exchange /Depository to whom said incident has been assigned for handling as per this SOP.

Notice of disablement, if any, as per above penalty structures in Table 3 and 5 sent to member shall also be communicated to its clients and other MIIs.

- Notwithstanding anything contained above, the Exchange and Depository Joint committee can, based on the nature of the incidence, prescribe an immediate & independent audit of the systems of the Trading Members/DP, and direct the Trading Members/DP to submit such reports as it deems fit.

7. Related Documents / References

- SEBI Circulars
- Exchange and Depository Notices, Guidelines and Advisories
- SOP document BSE/MEM/CIR/1.0, dated MARCH 11, 2025
- Annexure I

8. Procedure for Document Review/Revision

- Reporting
- Inter-MII reporting
- SEBI – Regulatory reporting
- Owner of the document/HOD should maintain the soft/hard copy of the document change or review request.
- Approved document change/Review request should be forwarded to the Owner of the document for review and approval.
- If the document owner accepts Proposed Change, then all controlled copy, master copy of concerned old document should be obtained from all the persons holding such copies if any, to prevent unintended use of obsolete documents.
- If the document owner accepts Proposed Change, then all controlled copy, master copy of concerned old document should be obtained from all the persons holding such copies if any, to prevent unintended use of obsolete documents.
- Document for which newer version is in place should be identified as “Obsolete Document” file. The owner may keep such a copy for reference for specified periods of time (2 years).
- The signature of the person returning controlled copies of old documents should be taken in Document Distribution Register.

- Approved changes should be incorporated in the Master copy of the document concerned.
- Revision date, revision number and change details should be updated at designated place on revised Master copy of document.
- Revised Master copy of documents should be approved by approving and issuing authority at designated place. Master Copy stamp should be affixed on revised Master Copy of document.
- Document Change/Review Request, which has a major impact on the process or requires additional resources to be allocated, should be brought before the Management Review Meeting for review & discussion.
- Owner should maintain all Document change/Review Request filed Date wise in Document change request file.
- Annual Review: All documents and formats of records to be reviewed by management at the end of each year (first year to be taken as beginning from the date of implementation) to ensure their suitability.