METROPOLITAN STOCK EXCHANGE

Department: Technology	**Segment: All Segments**
Circular No: MSE/IT/16598/2025	**Date: January 10, 2025**

Subject: Standard Operating Procedure (SOP) for handling Cyber Security Incidents

To All Members,

SEBI vide its circular EBI/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), accordingly the indicative scope for preparing Standard Operating Procedure (SOP) for handling Cyber Security incidents has been updated.

NSE in co-ordination with other Exchanges and Depositories have incorporated modifications in the above indicative scope, which is attached at **Annexure A.**

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

Precautionary Measure/Action:

- The connectivity between the RE/Trading Member/DP and Exchanges/Depositories– COLO/POP/SFTP/API, shall be kept disabled, in case of CRITICAL or HIGH severity cyber incidents.

- The connectivity shall be restored, ONLY once the trading RE/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 networks through Exchange/Depository connectivity of the Trading Member."

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

Table 1

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	Interim Report*	T#+3 Days
4	Mitigation Measure Report**	T#+7 Days*
5	Root Cause Analysis (RCA)*** report along with recommendations from Technology Committee of the RE	T#+30 Days##
6	Forensic Audit Report (on the incident) and its closure report****	Refer clause Forensic Investigation/ Audit given below****
7	Vulnerability Assessment and Penetration Testing (VAPT) for cyber incident and its closure reports	T#+45 days
8	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 provided by SEBI 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, and the steps taken to initiate the process of response and recovery.

** Mitigation Measure Report to describe immediate action taken by the Member/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. Additionally, it should also include time when operations/ functions/ services were restored and in the event of a disaster, time when disaster was declared.

****Forensic Investigation/ Audit**

1. For all incidents classified as High or Critical, the RE shall submit a forensic audit/ investigation report.
2. For incidents classified as low or medium, forensic report shall be submitted if the RCA is inconclusive or if the SEBI/ HPSC-CS directs the same.
3. After the completion of forensic audit, RE 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 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 by SEBI.
4. For all the issues/ observations submitted in the forensic report, the RE 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 RE shall file a closure report for the same after review (of the report) by respective *IT Committee for REs*.
5. In case the issues are not fixed within the prescribed timeline, appropriate regulatory action may be taken by SEBI as deemed fit depending on the nature of incident.

The penalty framework as applicable in case of delay / non submission of Immediate Cyber Incident, Mitigation Report, RCA, VAPT Report & Forensic Audit Report as stated in Table 1 above**,** is attached provided in Annexure **B**.

In addition to above, considering the severity of the cyber security incident (viz; Critical / High / Medium), number of active clients with the said Member/RE (viz; equal to or greater than 50,000 active UCC clients as on March 31) and such other parameters as defined from time to time, the matter may be placed before the Joint / Relevant Committee of the Exchange(s). The Penalty framework as applicable based on review of the cyber security incidents by the Joint / Relevant Committee of the Exchange(s) is attached at **Annexure C**.

The provisions of this SOP/Circular shall be applicable for all the cyber incidents as reported from January 20, 2025 and onwards.

All Trading Members/RE's are requested to take note of the above and comply.

For and on behalf of
Metropolitan Stock Exchange of India Limited

Laxmi Narayan Sahu
Chief Information Security Officer

Annexure A

SOP for handling Cybersecurity Incidents reported by SEBI Regulated Entities (REs)

As per Notification No. G.S.R 20(E) dated January 16, 2014, Rule (2) (h) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 defines "Cyber Security Incident" as under:

"Cyber Security Incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;"

1. Threshold for classifying incidents: Any incident stated under CERT-In Cybersecurity directions and meeting below criteria shall be mandatorily reported within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents:
   i. Cyber incidents of severe nature (such as Denial of Service, Distributed Denial of Service, intrusion, spread of computer contaminant including Ransomware) on any part of the public information infrastructure including backbone network infrastructure
   ii. Data Breaches or Data Leaks
   iii. Large-scale or most frequent incidents such as intrusion into computer resource, websites etc.
   iv. Cyber incidents impacting safety of human beings

   Further, "Cyber Security Breach" shall be defined as any incident or security violation that results in unauthorized or illegitimate access or use by a person as well as an entity, of data, applications, services, networks and/or devices through bypass of the underlying cyber security protocols, policies and mechanisms resulting in the compromise of the confidentiality, integrity or availability of data / information maintained in a computer resource or cyber asset. A cyber security breach is a subset of cyber security incident". It may be mentioned that this SOP is applicable to the cyber incidents reported by SEBI regulated REs directly, or by CERT-In, or by NCIIPC, or by MII's or by SEBI or any government agency, as occurred at SEBI regulated REs.

2. REs shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Such policy shall be approved by Board/Partners/Proprietor of the RE, as the case may be and shall be reviewed at least annually.
   All REs shall formulate an up-to-date Cyber Crisis Management Plan (CCMP) in line with national CCMP of CERT-In. CCMP shall be approved by Board/ Partners/ Proprietor of REs. Further, all REs shall develop an Incident Response Management Plan as part of their CCMP.

3. Cybersecurity incidents may be classified into the following four categories:

i) Critical Severity
ii) High Severity
iii) Medium Severity
iv) Low Severity

The parameters for classification of the incidents are as follows:

Table 2

Sr. No.	Category	Details
1	Low	System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malwares easily handled by antivirus software, etc.
2	Medium	Target recon or scans detected; penetration or Denial of Service attacks attempted with no impact on operations; widespread instances of known malwares easily handled by antivirus software; isolated instances of a new malwares not handled by anti-virus software; instances of phishing emails that were not recognized by employees and were clicked by them; instances of data corruption, modification and deletion being reported, etc.
3	High	Penetration or Denial of Service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software; unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials and MII official in email communications; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.
4	Critical	Successful penetration or Denial of Service attacks detected with significant impact on operations; ransomware attack; exfiltration of market sensitive data; widespread instances of data corruption causing impact on operations; significant risk of negative financial or public relations impact, large-scale data breach and any such adverse incidents which do not hamper the normal business operations but dent the overall cybersecurity posture of the organization etc.

Any incident that results in disruption, stoppage or variance in the normal functions/operations of systems of the entity thereby impacting normal/regular service delivery and functioning of the entity, must be classified as High or Critical incident.

4. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.

5. REs shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In). Additionally, any entity whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC), should report the incident to NCIIPC.

6. REs shall provide the reference details of the reported Cyber Security incident with CERT-In to the respective MIIs and SEBI. REs shall also provide details, regarding whether CERT-In team is in touch with the RE for any assistance on the reported Cyber Security incident. If the Cyber Security incident is not reported to CERT-In, REs shall submit the reasons for the same to the respective MIIs and SEBI. REs shall communicate with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.

7. REs shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, details need to be provided to the respective MIIs and SEBI. If no, then the reason for not registering complaint shall also be provided to respective MIIs and SEBI.

8. The details of the reported Cyber Security incident and submission to various agencies by the REs shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of SEC-MIRSD, TPD-MIRSD and CISO of SEBI.

9. Any cyber-attack(s), cybersecurity incident(s) and breach(es) experienced by REs falling under CERT-In Cybersecurity directions shall be notified to SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the email ID ***mkt_incidents@sebi.gov.in*** and group email ID of all MII's- member.cir@bseindia.in within 6 hours and SEBI Incident Reporting Portal within 24 hours. Stockbrokers/ Depository Participants shall also report the incident(s) to Stock Exchanges/ Depositories along with SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. Any/ all other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) within 24 hours. It may be noted that in case any RE does not report a cybersecurity incident to SEBI (when the RE is/ was aware of the incident) in a manner as laid down in the applicable cybersecurity framework, appropriate regulatory action may be taken as deemed fit depending upon the nature of the incident.

10. In case if the incident occurs in a particular business function of the RE, the RE will have to inform the MII of that business function e.g., in case the incident is in the Depository function of the RE, the RE will have to inform the respective Depositories with whom it is registered.
11. During the life cycle of incident handling, the following aspects need to be broadly covered/captured:
    a. Whether the RE has followed the incident response plan of their organization while handling the incident.
    b. Whether the RE has taken necessary (immediate) measures to contain the incident impact.
    c. Whether the RE has communicated to all relevant stakeholders about the incident.
    d. Whether RE has taken sufficient measures to control, mitigate and remediate the incident.
    e. Whether Root cause analysis (RCA) has been performed by RE.
    f. Whether lessons learnt have been implemented by RE.
    g. Whether the issues/loopholes identified in RCA stage have been addressed/plugged by the RE.
    h. Whether RE has hired any independent agency to conduct IS Audit/ forensic audit related to the incident (as per applicability).
    i. Whether RE has addressed/plugged vulnerabilities identified in the audit mentioned in point h above.

12. The RCA, forensic audit, VAPT reports shall be reviewed by the respective IT Committee for REs before the reports are submitted to SEBI/Exchanges/Depository/MIIs. A report on the review conducted/ recommendations provided by IT Committee for REs shall also be submitted to SEBI/Exchanges/Depository/MIIs along with the reports mentioned in Table No. 1. Further, the vulnerabilities identified in VAPT shall be closed within 3 months from the submission of report. REs are also expected to maintain risk register which shall be reviewed by the IT Committee for REs."

13. SEBI shall examine the incident on the basis of reports submitted. Further, RE shall classify the cybersecurity incident based on its severity as per Table No 2 and the same shall be reviewed by respective IT Committee for REs of the RE before the reports are submitted to SEBI/Stock Exchanges/Depositories/MIIs. Cybersecurity incidents occurred at Qualified RE's and categorized as Critical or High which has high impact & has a broad reach for such incidents qualified REs shall issue a press release within a one working day from the intimation of normalcy of operation to Exchange. The press release shall include (but not limited to) a brief of the incident, actions taken to recover, normal operation resumption status (once achieved), etc. and inform all the affected customers/ stakeholders. In case of any delay in issuance of PR by qualified RE's penalty shall be applicable as per Table – 3.

14. In case the reports are found to be deficient or inaccurate in any manner (for instance no identification or incorrect identification of root cause, inaccurate sequence of events, etc.), appropriate regulatory action may be taken as deemed fit depending upon the nature of the incident. RE may be provided an additional time upto 15 days from the day of being notified of the deficiency/ inaccuracy, for submitting the accurate and complete report.

15. In the event of RE not submitting accurate and complete reports after being provided additional time, appropriate regulatory action may be taken as deemed fit depending upon the nature of the incident (over and above the action mentioned in clause 14 above).

16. Critical or High category of cybersecurity incidents experienced by Qualified REs, and Mid-size REs shall be mandatorily put up for the review for HPSC-CS. Remaining incidents i.e., low and medium for all REs, and high and critical severity incidents for small-size and self-certification REs shall be processed by SEBI internally. The review by HPSC-CS and SEBI shall be as follows:

17.1 Review of Critical or High category of cybersecurity incidents in Qualified and Mid-Size REs

i. For critical/high category incidents, SEBI may confirm the severity or recommend a different severity on the basis of its analysis.

ii. SEBI may examine the reports, review the severity of the incident and provide its recommendations on the same.

iii. Further, if the SEBI determines that the incident occurred on account of non-compliance of SEBI cybersecurity framework/ advisories, appropriate regulatory action may be taken on the RE notwithstanding any action levied above.

iv. The recommendations of the SEBI shall be implemented by the RE in a time-bound manner. The timelines for the implementation shall be decided by the committee based on the discussion with relevant stakeholders (i.e. SEBI and the RE).

v. RE may be required to submit audit report(s) to verify the implementation of committee's recommendations.

17.2 Review of other cyber incidents

i. Cyber incidents not falling under category mentioned in Para 17.1, may be examined by SEBI/MII on the basis of the documents submitted by the RE).

ii. Further, if it is determined that the incident occurred on account of non-compliance of SEBI/MII cybersecurity framework/ advisories, appropriate regulatory action may be taken on the RE notwithstanding any action levied above.

iii. RE shall formulate a remediation and mitigation plan. The timelines for implementation of the measures shall also be decided based on the discussions (between SEBI/MII and RE).

Annexure B

In case, Non-submission of Cyber Incident, Mitigation Report, RCA, Forensic Audit Report, VAPT Report as stated under **Table 1** are not submitted within the timelines, following penalties shall be applicable to such Members: -

Table-3

Sr. No.	**Penalty for not submitting the above reports within due date**	**For All Members/ DPs (other than QSB/QREs)**	**For QSB/QRE Members**
1	Non-submission of Cyber Incident reporting (Immediate Submission) within the time (within 6 hours) specified by the Exchange.	If the incident 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 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	Charges per day for first 7 calendar days or till submission Mitigation Report, RCA, Forensic Audit Report & VAPT Report whichever is earlier.	Rs. 1500 per day	Rs. 3000 per day
3	Charges per day from 8th calendar day to 21st calendar day or submission Mitigation Report, RCA, Forensic Audit Report & VAPT Report whichever is earlier.	Rs. 2500 per day	Rs. 5,000 per day
4	In case of non-submission within 21 calendar days from the due date of submission Mitigation Report RCA, Forensic Audit Report & VAPT Report	New Client registration to be prohibited and notice of 7 days for disablement of trading facility shall be issued. The disablement notice issued to the member/ DP will be shared with all the MII's for information.	
5	In case of non-submission within 28 calendar days from the due date of submission Mitigation Report RCA, Forensic Audit Report & VAPT Report	Member/DP shall be disabled in all segments till receipt of complete submission.	
6	In case press release is not issued within a one working day from the intimation of normalcy of operation to Exchange(s)/Depositories. (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 to whom said incident has been assigned for handling as per this SOP.

Annexure C

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

1.In case the reports (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 non-compliance of SEBI cyber security policies and guidelines, penalties as prescribed under **Table 4** below shall be applicable to such Members/ DPs: -

Table- 4

Particulars	**Penalty Amount for All Members / DPs (other than QREs/QSBs)**	**Penalty Amount for QREs/QSBs Members**
In case the reports (as stated under Table 1) 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
In case the report is found to be misleading or inaccurate	Rs 1,00,000/- per misleading or inaccurate component	Rs 2,00,000/- per misleading or inaccurate component
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/-
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 noncompliance	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.

2. 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" shall be followed from the expiry of the deadline specified by Joint / Relevant Committee of Exchange(s)/Depositories: -

Table 5

Sr. No.	**Penalty in case of delay beyond the deadline as specified by Joint / Relevant Committee of MIIs/Exchange(s)/Depositories**	**For All Members (other than QSBs/QREs)**	**For QSBs/QREs Members**
1	Charges per day for first 7 calendar days or till submission of report, 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, 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 due date of submission	New Client registration to be prohibited and notice of 7 days for disablement of trading facility shall be issued. The disablement notice issued to the member will be shared with all the Exchanges/Depositories for information.	
4	In case of non-submission/non implementation of recommendations of Joint/Relevant Committee of Exchange(s)/Depositories within 28th calendar day from the due date of submission	Member/DP shall be disabled in all segments till receipt of complete submission / closure of non-compliance.	

Note: 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, 4 and 5 sent to member shall also be communicated to its clients and other MIIs.