National Stock Exchange of India Limited

Circular

DEPARTMENT: INSPECTION	
Download Ref No: NSE/INSP/53387	**Date: August 23, 2022**
Circular Ref. No: 59/2022	

To All Members,

Sub: Modification in Cyber Security and Cyber resilience framework for Stock Brokers

This is with reference to SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and Exchange Circular Ref. No.: NSE/ITRC/40081 dated January 30, 2019 on "Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants".

SEBI has issued Circular No. SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022, wherein they have provided partial modification to Annexure – 1 of SEBI Circular dated December 03, 2018 (paragraph 52). A copy of the said circular is enclosed as **Annexure A**.

In view of the modification to paragraph 52 of Annexure – 1 of SEBI Circular dated December 03, 2018, point nos. 3 & 7 of the indicative scope as provided for preparing of Standard Operating Procedure (SOP) for handling Cyber Security incidents issued vide Exchange Circular NSE/INSP/48163 dated May 03, 2021 stands modified and shall be read as under (updated version attached at **Annexure B**)

> *3. Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Members, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.*
>
> *7. The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events, all Cyber-attacks, threats, cyber-incidents and breaches experienced by Members to NSE (in manner specified by NSE) & SEBI (on the dedicated email ID sbdp-cyberincidents@sebi.gov.in) within 6 hours of noticing / detecting such incidents or being brought to the notice about such incidents as well as submit the quarterly reports containing the information on cyber-attacks, threats, cyber-incidents and*

National Stock Exchange of India Limited

breaches experienced by Stock Brokers and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges / Depositories and SEBI shall be submitted to Stock Exchanges within 15 days after the end of the respective quarter in the manner as specified by NSE from time to time.

As per modified para 42 prescribed under SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022: -

"Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity…"

With respect to the above provision, Stock Exchanges in consultation with SEBI, hereby clarify that the VAPT shall be carried out and completed during the period September to November of every financial year and the final report on said VAPT shall be required to be submitted to the Stock Exchanges within one month from the date of completion of VAPT after approval from Technology Committee of respective Stock Brokers.

Members are advised to take note of the contents of the Circular and comply.

For and on behalf of
National Stock Exchange of India Limited

Chirag Shah
Senior Manager

National Stock Exchange of India Limited

In case of any clarifications, Members may contact our below offices:

Regional Office	E MAIL ID	CONTACT NO.
Ahmedabad (ARO)	inspectionahm@nse.co.in	079- 49008632
Chennai (CRO)	inspection_cro@nse.co.in	044- 66309915 / 17
Delhi (DRO)	delhi_inspection@nse.co.in	011- 23459127 / 38 / 46
Kolkata (KRO)	inspection_kolkata@nse.co.in	033-4040 0412/59
Mumbai (WRO)	compliance_wro@nse.co.in	Board Line: 022-25045000 / 022-61928200 Direct Line: 022-25045138 / 022-25045144 Extn: 28144/28138
Central Help Desk	compliance_assistance@nse.co.in	

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/TPD/P/CIR/2022/93 **June 30, 2022**

To

All Recognized Stock Exchanges and Depositories

Dear Sir/ Madam,

Sub: - Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants

1. SEBI vide circular dated 03 December 2018, 15 October 2019 and 07 June 2022 prescribed framework for Cyber Security and Cyber Resilience for Stock Brokers / Depository Participants.

2. In partial modification to Annexure 1 of SEBI circular dated December 03,2018 the paragraph-52 shall be read as under:

> *52. All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents.*
>
> *The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.*
>
> *The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and*

attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges /Depositories and SEBI shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year. The above information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.

3. Stock Brokers / Depository Participants shall take necessary action for implementation of the circular.

4. Stock Exchanges and Depositories shall;
   a) make necessary amendments to the relevant byelaws, rules and regulations for the implementation of the above direction and
   b) bring the provisions of this circular to the notice of their members/participants and also disseminate the same on their websites.

5. The provisions of the Circular shall come into force with immediate effect.

6. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully,

Vishal M Padole
Deputy General Manager
MIRSD
Tel. No: 022 26449247
Email ID: vishalp@sebi.gov.in

Annexure B

1. Members shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Such policy shall be approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and shall be reviewed annually by the "Internal Technology Committee" as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy.

2. Members shall examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.

3. Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Members, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

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

5. Members 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 Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.

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

7. The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events, all Cyber-attacks, threats, cyber-incidents and breaches experienced by Members to NSE (in manner specified by NSE) & SEBI (on the dedicated email ID sbdp-cyberincidents@sebi.gov.in) within 6 hours of noticing / detecting such incidents or being brought to the notice about such incidents as well as submit the quarterly reports containing the information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges / Depositories and SEBI shall be submitted to Stock Exchanges within 15 days after the end of the respective quarter in the manner as specified by NSE from time to time.