Metropolitan Clearing Corporation of India Limited

Department: Information Technology	**Segment: All**
Circular No: MCCIL/IT/2164/2022	**Date: February 28, 2022**

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

To All Members,

This is with reference to the SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 on Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants, the various Exchanges & Clearing Corporations issued the circulars thereunder and SEBI Directives, requiring Member Brokers / Participants / Intermediaries to maintain Standard Operating Procedures (SOP) to handle of Cyber Security Incidents.

As per SEBI's directive, all Members shall maintain a Standard Operating Procedure (SOP) with respect to handling of Cyber Security incidents. Members are hereby advised to prepare the SOP on handling and reporting of Cyber Security incidents as indicated below:

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 Actions/ Responses for Cyber Security incidents based on severity.

3. Members shall report Cyber Security incidents to Indian Computer Emergency Response Team (CERT-In).

4. Members shall provide the reference details of the reported Cyber Security incident with CERT-In to the Exchange, Clearing Corporation 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.

5. 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.

6. 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, Clearing Corporation and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.

7. 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.

8. 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 within 24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter.

For any clarifications, contact Customer Service on 022-68316600 or send email to MCCIL INFO <info@mclear.in>

For and on behalf of
Metropolitan Clearing Corporation of India Limited

Sumit P. Badakh
Chief Information Security Officer