Circular No.: NSDL/POLICY/2021/0124 December 17, 2021

Subject - SEBI Advisory regarding Cyber Security - Prevention of DDoS Cyber-attacks and Cyber Security preparedness

Attention of Participants is invited to SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 (NSDL circular no. NSDL/POLICY/2018/0069 dated December 6, 2018) regarding Cyber Security & Cyber Resilience framework of Depository Participants. Participants were communicated vide Circular Nos. NSDL/POLICY/2020/0047 & NSDL/POLICY/2020/0126 dated April 9, 2020 & September 20, 2020 regarding Cyber Security Advisory from National Critical Information Infrastructure Protection Centre (NCIIPC) to take requisite precautions & SEBI advisory on Cyber Security - Prevention of DDoS Cyber-attacks and Cyber Security preparedness respectively.

SEBI has vide its email dated November 11, 2021 regarding Cyber Security Advisory w.r.t. Distributed Denial of Service (DDoS) attacks on system of intermediaries, informed that as financial services is a critical information infrastructure, it has been observed that it is one of the primary targets of cyber-attacks and recently one of the major intermediary has reported multiple DDoS attacks on its systems.

In order to ensure continuous availability of services and to prevent cyber-attacks, Participants are once again requested to ensure the following:

1. Systems to be put in place for creating a robust cyber security and cyber resilience framework in order to counter various types of cyber-attacks
2. Review the cyber security safeguards put in place, and any gaps found should be fixed on priority.
3. Ensure adequate safety and security measures (like intrusion detection/prevention system, anti-virus, firewall, etc.) are in place to protect the critical data, infrastructure and applications.
4. Review the communication links provisioned for trading, communications and other services exposed to the customers and partners on the internet /private networks. Ensure that all the internet links and services are adequately protected from cyber-attacks including DoS / DDoS attacks.
5. Continuously monitor the applications and services for their availability and response time.
6. Any cyber security incident is to be promptly reported to the relevant authorities.

Further, Participants shall ensure adherence to cyber security guidelines / advisories issued by SEBI, follow best industry practices and comply with other guidelines issued by CERT-In and NCIIPC from time to time.

Participants are requested to take note of the above and ensure compliance.

For and on behalf of
National Securities Depository Limited

Gayak Jalan
Manager

FORTHCOMING COMPLIANCE			
Particulars	**Deadline**	**Manner of sending**	**Reference**
Investor Grievance Report (Monthly)	By 10th of the following month.	Through e-PASS	Circular No. NSDL/POLICY/2015/0096 dated October 29, 2015

Digitally signed by
Name : GAYAK JALAN
Date : 17-12-2021 17:40:48
Reason : Authentication