Circular No.: NSDL/POLICY/2020/0143 October 30, 2020

Subject: SEBI Advisory regarding Remote Access and Telecommuting

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 respectively 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.

In accordance with SEBI email dated October 22, 2020 regarding advisory on Remote Access and Telecommuting, Participants are advised as under:

1. Ensure proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.
2. For implementation of the concept of trusted machine as end users, categorize the machines as official desktops / laptops and accordingly the same may be configured to ensure implementation of solution stack considering the requirements of authorized access. Official devices shall have appropriate security measures to ensure that the configuration is not tampered with. Participants shall ensure that internet connectivity provided on all official devices shall not be used for any purpose other than the use of remote access to data centre resources.
3. If personal devices (BYOD) are allowed for general functions, then appropriate guidelines should be issued to indicate positive and negative list of applications that are permitted on such devices. Further, these devices should be subject to periodic audit.
4. Implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder’s claimed identity.
5. Ensure that the trusted machine is the only client permitted to access the data centre resources. The Participants shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.
6. Explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. Participants shall implement short session timeouts for better security. Towards this end, it is suggested that the Participants may consider running a mandatory monitor on the device that executes:
   a. At random intervals takes a picture with the webcam and uploads the same to the Participant’s server,
   b. At random intervals pops up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the Participants server as a security event.
7. Ensure that appropriate risk mitigation mechanisms are put in place whenever remote access of data centre resources is permitted for service providers.

8. Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the Participants shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.
9. Ensure that the backup, restore and archival functions work seamlessly, particularly if the users have been provided remote access to internal systems.
10. Exercise sound judgement and discretion while applying patches to existing hardware and software and apply only those patches which were necessary and applicable.
11. The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture.
12. Update its incidence response plan in view of the current pandemic.
13. Implement cyber security advisories received from SEBI, MII, CERT-IN and NCIIPC on a regular basis.
14. Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness.

Participants are requested to take note of the above and ensure compliance. Participants are requested to provide their feedback for the above advisory, if any, by November 20, 2020 at dpinfosec@nsdl.co.in.

For and on behalf of
National Securities Depository Limited

Chirag Shah
Senior 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
Networth Certificate and Audited Financial Statements for the FY 2019-20	October 31st , 2020	By hard copy to Inspection Department	Circular No. NSDL/PI/98/414 dated September 1, 1998 Circular No. NSDL/POLICY/2020/0131 dated September 30, 2020
Risk Assessment Template (April - September)	October 31st, every year	Through e-PASS	Circular No. NSDL/POLICY/2018/0050 dated September 25, 2018
Internal/ Concurrent Audit Report (April - September)	November 15th every year	Through e-PASS	Circular No. NSDL/POLICY/2020/0136 dated October 19, 2020

Digitally signed by
Name : Chirag Shah
Date : 30-10-2020 15:55:29
Reason : Authentication