

All Segment

Circular No. : MCCIL/IT/1803/2020

October 30, 2020

Subject: Cyber Security Advisory - Remote Access and Telecommuting

In terms of the provisions of the Rules, Bye-Laws and Regulations of the Metropolitan Clearing Corporation of India Limited (MCCIL), Clearing Members of the MCCIL are notified as under:

There are news reports that cyber criminals around the world are capitalizing on the Covid-19 crises by exploiting the remote working vulnerabilities on computers, routers and unprotected home networks. A cyber-attack on critical devices, data or network links may be devastating and cause infrastructure failures. Hence it is advised that we should be vigilant and follow the Cyber Security Guidelines issued by SEBI and the best practices and advisories issued by the CERT-IN and NCIIPC, as given in the **Annexure**.

Members are requested to formulate the appropriate Standard Operating Procedures (SOP) and thereby ensure safety by keeping a close watch on their IT infrastructure for timely detection and prevention of cyber-attacks. For clarifications, members may send an email to mccil_infosec@mcclar.in.

Sec_rity is incomplete without U!

For and on behalf of
Metropolitan Clearing Corporation of India Limited

Mr. Sumit Badakh
IT Head & CISO

Metropolitan Clearing Corporation of India Limited

Regd. Office: 4th Floor, Vibgyor Towers, Opp. Trident Hotel, Plot No. C62, Bandra Kurla Complex, Bandra (East), Mumbai - 400 098
Tel: +91-22-6112 9000 • Fax: +91-22-2652 5731 • URL: www.mcclear.in • Email: info@mcclear.in • CIN: U67120MH2008PLC188032

Annexure

Below are measures regarding remote access and telecommuting taking into consideration the current COVID-19 situation:

- 1) The intermediaries shall have 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, the intermediary shall 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. The intermediary 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) The intermediary shall 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) The intermediary shall ensure that the trusted machine is the only client permitted to access the data centre resources. The intermediary 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) The intermediary shall 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. The intermediary shall implement short session timeouts for better security. Towards this end, it is suggested that the intermediary may consider running a mandatory monitor on the device that executes:
 - a) At random intervals take a picture with the webcam and upload the same to the intermediary's server.

Metropolitan Clearing Corporation of India Limited

Regd. Office: 4th Floor, Vibgyor Towers, Opp. Trident Hotel, Plot No. C62, Bandra Kurla Complex, Bandra (East), Mumbai - 400 098

Tel: +91-22-6112 9000 • **Fax:** +91-22-2652 5731 • **URL:** www.mclear.in • **Email:** info@mclear.in • **CIN:** U67120MH2008PLC188032

- b) At random intervals pop up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the intermediary server as a security event.
- 7) The intermediary shall 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 intermediary shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.
 - 9) The intermediary shall ensure that the backup, restore and archival functions work seamlessly, particularly if the users have been provided remote access to internal systems.
 - 10) The intermediary is advised to 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) The intermediary shall update its incidence response plan in view of the current pandemic.
 - 13) The intermediary shall 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.