



# KK SECURITIES LIMITED

Member : National Stock Exchange of India Ltd. (CM, F&O and Currency)

Member : BSE Ltd. (CM, F&O)

Member : Metropolitan Stock Exchange Ltd. (CM, F&O)

Participant : National Securities Depository Ltd.

CIN : U74899DL1994 PLC060238

20  
Regd. Office : 76-77, Scindia House, 1st Floor,  
Janpath, Connaught Place, New Delhi-110 001  
Tel.: 23722916, 46890000 (25 Lines)  
Fax : 011-23723571 Email : kksl@kksecurities.com

## Remote Access & Telecommuting Policy

Exchanges under advisory of SEBI have issued circular on threats emanating from work-from-anywhere model through remote access and telecommuting and to ensure continuous availability of services requested implementation of safety features by members. The compliance of the same is as under:

KK Securities Ltd. shall :-

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. It shall implement the concept of trusted machine as end users, categorize the machines as official desktops / laptops and accordingly the same shall be configured to ensure implementation of solution stack considering the requirements of authorized access. All official devices shall have appropriate security measures to ensure that the configuration is not tampered with. It 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. Personal devices may be allowed for general functions using appropriate guidelines indicating 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.
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. It will, if feasible, implement suitable mechanisms 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. Measures such as video-recognition, short session timeouts, random intervals pops up and prompts biometric authentication, cameras and security guards shall be considered.
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 to be monitored continuously for any abnormal access and appropriate alerts and alarms generated.
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 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.

12. Implement cyber security advisories received from SEBI, MII, CERT-IN and NCIIPC on a regular basis.

**This policy was approved at the Board meeting of KK Securities Ltd. held on February 16, 2024.**

**For Board of Directors of KK Securities Limited**

**(Mukesh Rustagi)**



**Director Corp., Compliance Officer & Principal Officer**

**Dated : 16/02/2024**

**Place : New Delhi**