Circular no.: MCX/TECH/145/2026 March 23, 2026

Security Requirements for Members Connecting Through MCX SSL VPN Solution

In terms of provisions of the Rules, Byelaws and Business Rules of the Exchange and in continuation of circular No. MCX/TECH/587/2025 dated November 14,2025, MCX/TECH/206/2025 dated April 25,2025, MCX/TECH/231/2025 dated May 2,2025, MCX/TECH/466/ 2025 dated September 18, 2025, MCX/TECH/587/2025 dated November 14, 2025, MCX/TECH/038/2026 dated January 23, 2026 and MCX/TECH/127/2026 dated March 13,2026. Members are requested to notify as under.

The Exchange has received a request from its members to extend the timeline for discontinuing **VPN support on Windows 10**. Accordingly, the Exchange has decided to extend the timeline until the close of business hours of 28th March 2026.

To ensure the safety of the MCX trading environment, all members connecting through SSL VPN solution from internet mode of connectivity must adhere to the following security requirements:

Minimum Desktop Security Requirements

- All members are required to use Windows 11 to continue accessing VPN services post 28th March 2026.
- Use only licensed and updated operating systems for trading activities.
- Ensure the operating system and all applications, including the SSL VPN client, are patched with the latest security updates.
- Install, activate, updated and reputed end point security solution. Daily scans of the desktops are strongly recommended.
- Disable all unnecessary services and unlicensed software.
- Ensure operating system firewall is enabled in the desktop.
- Ensure user rights are properly set in the desktops for login to VPN client.
- Members are requested to follow the SOP mentioned in circular No. MCX/TECH/206/2025 dated April 25,2025 for login to VPN Client

VPN and Network Best Practices

- Activate VPN before accessing MCX trading systems through Internet mode of connectivity.
- Keep VPN software updated as and when MCX releases the same to mitigate risks from newly discovered vulnerabilities.
- Avoid using public Wi-Fi network.
- Ensure to report MCX whenever there is change in mobile OTP client user and/or handset.

Additional Cybersecurity Measures

- Use strong, unique passwords for MCX and related trading accounts.
- Do not use the desktop for browsing unrelated websites or downloading untrusted files.

Compliance and Monitoring

- MCX reserves the right to audit member security compliance at any time.
- Non-compliance with the above security requirements may result in connection issues to trading system.

It is requested to adhere to the above-mentioned requirements to safeguard overall integrity and security of Members and the MCX trading platform.

Members are requested to take note of the same.

Shivanand Jogade
AVP Technology

Kindly contact Customer Support on 022 - 6649 4040 or send an email at customersupport@mcxindia.com for further clarification.