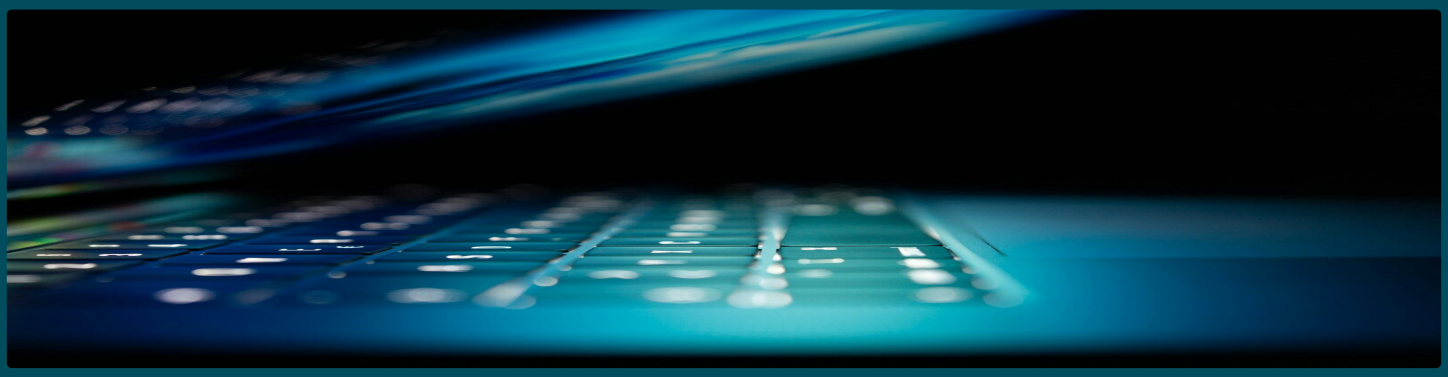
INDIALAW



REGULATORY

MCX Circular: Information Sharing on Cybersecurity Incidents

Circular No. MCX/TECH/179/2026 | Dated: April 6, 2026 | Effective Deadline: April 15, 2026 I. Background and Regulatory Context The Multi Commodity Exchange of India Limited (“MCX” or “the Exchange”) has, by way of Circular No. MCX/TECH/179/2026 dated April 6, 2026, issued a formal directive requiring all trading members to report Cyber Security Incidents for the quarter […]

AUTHOR Aditi Rana, Tanvi Dalvi

PUBLISHED 9 April 2026

Circular No. MCX/TECH/179/2026 | Dated: April 6, 2026 | Effective Deadline: April 15, 2026

I. Background and Regulatory Context

The Multi Commodity Exchange of India Limited ("MCX" or "the Exchange") has, by way of Circular No. MCX/TECH/179/2026 dated April 6, 2026, issued a formal directive requiring all trading members to report Cyber Security Incidents for the quarter ending March 31, 2026. This directive is issued in exercise of the powers conferred upon the Exchange under its Rules, Bye-Laws, and Business Rules, and constitutes a continuation of a series of regulatory communications on the subject of cybersecurity governance, commencing with Circular No. MCX/TECH/524/2018 dated December 13, 2018.

The issuance of this Circular underscores the Exchange's sustained commitment to fortifying the cybersecurity framework governing commodity derivatives markets in India. It reflects a broader regulatory philosophy increasingly prevalent across financial market infrastructure that treats cyber resilience not merely as a technical obligation, but as a fundamental pillar of market integrity and investor confidence.

Table of contents

- I. Background and Regulatory Context
- II. Nature and Scope of the Reporting Obligation
- III. Cross-Exchange Reporting Mechanism: A Significant Procedural Development
- IV. Consequences of Non-Compliance
- V. Advisory and Recommended Course of Action

II. Nature and Scope of the Reporting Obligation

Pursuant to the provisions of the Circular, all trading members of the Exchange are obligated to report Cyber Incidents irrespective of whether any such incident has in fact occurred during the relevant quarter. The mandatory nature of this disclosure, even in the absence of an actual incident (commonly referred to as a "nil reporting" obligation), is a significant feature of the regulatory design. It serves to ensure that the Exchange maintains a comprehensive and contemporaneous record of the cybersecurity posture of all market participants.

Such submissions are required to be made through the Exchange's designated digital portal at https://member.mcxindia.com . The portal shall remain accessible for the purpose of such submissions until April 15, 2026, thereby affording trading members a limited but defined compliance window.

III. Cross-Exchange Reporting Mechanism: A Significant Procedural Development

Of particular legal and procedural significance is the introduction of a technology-based cross-exchange submission mechanism, first articulated in Exchange Circular Ref. No. MCX/MEM/348/2025 dated July 18, 2025, and now reiterated in the present Circular. Under this framework, trading members who are registered with the National Stock Exchange of India Limited ("NSE") and are simultaneously registered with one or more of BSE, MSE, MCX, or NCDEX, are now required to submit their Cyber Security Incident details exclusively to NSE.

NSE shall thereafter transmit the relevant submissions to the respective Exchanges on behalf of the reporting members. This consolidated reporting framework represents a material rationalization of compliance obligations for multi-exchange participants, eliminating the erstwhile requirement of duplicate or parallel submissions to each Exchange. Members who are not registered with NSE remain unaffected by this provision and are required to continue making direct submissions to MCX through the existing process.

IV. Consequences of Non-Compliance

The Circular explicitly provides that non-compliant members shall render themselves liable for such action as may be deemed fit by the Exchange. While the Circular does not enumerate the specific sanctions applicable in the event of default, the Exchange retains broad disciplinary powers under its regulatory framework.

V. Advisory and Recommended Course of Action

In view of the foregoing, trading members of MCX are advised to take immediate cognizance of the obligations prescribed under Circular No. MCX/TECH/179/2026 and ensure timely compliance prior to the portal closure deadline of April 15, 2026. Members registered with NSE are advised to coordinate their submissions through NSE's designated mechanism, while members not registered with NSE must access and submit their reports directly on the Exchange's member portal.

For more details, write to us at:?contact@indialaw.in

References:

[Circular No.: MCX/TECH/179/2026] [April 06, 2026] Information sharing on Cyber Security Incident

Related Practice Areas

Regulatory & Compliance Advisory