INDIALAW

CYBER LAW

Fortifying the Digital Frontier: Decoding NCDEX’s 2026 Master Circular on Cyber Security Compliance

AUTHOR Appurv Bhatia, Tanvi Dalvi

PUBLISHED 20 April 2026

Introduction

On April 13, 2026, the National Commodity & Derivatives Exchange Limited (NCDEX) issued Master Circular No. NCDEX/Member Tech Compliance-007/2026, consolidating all operational cyber security compliance directives applicable to its members as of March 31, 2026. This Master Circular consolidates and operationalises the cyber security compliance obligations already issued by NCDEX and SEBI up to March 31, 2026, providing a unified reference framework.

Mandatory Cyber Incident Reporting

The circular reaffirms the obligation of all members to formally record and submit quarterly reports detailing cyber-attacks, threats, and mitigation measures experienced during each financial quarter. Such reports must be transmitted to the Exchange via the prescribed email address or the NSE Common Submission Portal within stipulated deadlines specifically, by the 15th day following the conclusion of each quarter. This framework, rooted in SEBI's circular of October 2019, serves the dual purpose of enabling institutional learning and ensuring regulatory visibility into the sector's evolving threat landscape.

Cyber Security and Resilience Audit Obligations

Members are further mandated to commission and submit digitally signed Cyber Security and Cyber Resilience Audit Reports at defined intervals. Type I and Type II Trading Members are subject to annual audits, whereas Type III Trading Members utilising NNF facilities, algorithmic trading, or Qualified Stock Broker (QSB) status must undergo half-yearly audits. The audit report is considered complete only when accompanied by management comments, and each non-compliance identified by the auditor must be remedied through a Corrective Action Taken Report (ATR) submitted within prescribed timelines. Non-submission or delayed submission attracts penal charges, reinforcing the binding nature of this obligation.

Vulnerability Assessment and Penetration Testing

The circular prescribes that Vulnerability Assessment and Penetration Testing (VAPT) be conducted annually during the period September to November, exclusively by agencies empanelled under CERT-In. The final VAPT report must be submitted to the Exchange within one month from the date of completion, following approval by the member's Technology Committee. Members are additionally required to conduct VAPT prior to the commissioning of any new internet-accessible system, thereby embedding security review as an integral component of system deployment governance.

SaaS Compliance and Cloud Governance

In recognition of the increasing adoption of cloud-based and Software-as-a-Service (SaaS) solutions, the circular directs members to confirm, on a half-yearly basis, whether specified categories of confidential data are hosted on SaaS platforms, in accordance with CERT-In advisory guidelines. Separately, a dedicated framework governs the adoption of cloud services by SEBI-regulated entities, requiring such entities to remain cognisant of the unique cyber security risks and governance challenges that cloud computing introduces. These provisions collectively reflect a regulatory awareness of the evolving digital infrastructure landscape.

Technical Glitches: Framework and Reporting

A detailed Standard Operating Procedure (SOP), effective January 9, 2026, governs the identification, reporting, and remediation of technical glitches in members' electronic trading systems. A "technical glitch" is defined as any malfunction in hardware, software, network, or bandwidth that results in a disruption to trading or risk management functions for a continuous period of five minutes or more. The SOP applies to IBT and STWT platform providers with more than 10,000 registered clients. Upon the occurrence of such a glitch, members are obligated to notify the Exchange and affected clients within two hours, file a Preliminary Incident Report by T+1, and submit a Root Cause Analysis within fourteen working days.

API Security, Authentication, and Vendor Obligations

The circular sets forth comprehensive API security standards applicable to Exchange-empanelled vendors and Application Service Providers. These standards mandate the maintenance of an API inventory, the deployment of strong mutual authentication mechanisms, centralised API gateway security, data encryption, input validation, rate limiting, and regular security assessments aligned with the OWASP Top 10 framework. Vendors are further required to conduct annual software audits in accordance with ISO 12207:2017 standards. The inclusion of vendor obligations within this master circular signals the Exchange's intent to extend compliance responsibility across the technology supply chain.

Two-Factor Authentication and Session Management

All members offering IBT and STWT platforms are required to implement Two-Factor Authentication (2FA) for every client login attempt. Of particular note is the requirement that active login sessions be mandatorily terminated at the end of each trading day, with subsequent access permitted only upon successful re-authentication. This provision addresses a systemic vulnerability whereby client sessions remained active across multiple trading days, thereby exposing investor accounts to unauthorised access.

Geo-Political Preparedness, CSK Onboarding, and the CSCRF

In response to heightened geo-political risks, the circular advises members to strengthen their Security Operations Centre (SOC) monitoring capabilities, act promptly on CERT-In and NCIIPC advisories, and remain vigilant against DDoS and ransomware threats. Additionally, stockbrokers with more than 50,000 active traded clients are required to register with the CERT-In Cyber Swachhta Kendra (CSK) platform. The circular also clarifies key provisions of SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF), including the methodology for computing registered client counts and the categorisation of proprietary stockbrokers for compliance applicability purposes.

Conclusion

The NCDEX Master Circular of 2026 constitutes a consolidated and enforceable compliance framework derived from existing regulatory mandates for cyber security governance in the commodity derivatives market. Its provisions touch every dimension of a member's technology operations from incident reporting and penetration testing to vendor management and client authentication.

Related Practice Areas

Statutory And Regulatory Compliance | Cybersecurity and Incident Response