NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to all trading and clearing members

Circular No	: NCDEX/Member Tech Compliance-010/2025
Date	: May 09, 2025
Subject	: Advisory on Cyber Security Preparedness for current Geo-Political Development

Given the prevailing geopolitical landscape, the threat posed by state and non-state actors to India's Critical Information Infrastructure (CII) and financial institutions has escalated significantly. These malicious entities are actively attempting to compromise the security of financial systems through various sophisticated attack vectors. Their objectives range from disrupting critical services and obstructing key networks—particularly via Distributed Denial-of-Service (DDoS) and ransomware attacks—to defacing and destabilizing digital infrastructure. Additionally, they seek to undermine the confidentiality, integrity, and availability (CIA) triad of financial entities, posing a severe risk to national security and economic stability.

In light of these challenges, it is imperative that organizations maintain a heightened state of vigilance and preparedness. Therefore, all entities must promptly implement the necessary safeguards and proactive measures to mitigate these threats effectively.

- Organizations must promptly act upon alerts and advisories issued by NCIIPC, CERT-In, SEBI, and other relevant regulatory bodies.
- Transition to an enhanced alert mode with round-the-clock Security Operations Center (SOC) and Network Operations Center (NOC) monitoring to ensure proactive threat detection and swift mitigation. Maintain near-total manpower availability to sustain a high state of operational readiness.
- Conduct regular, systematic log reviews of web servers and perimeter security devices—such as Web Application Firewalls (WAF), Firewalls, and DNS infrastructure
- Incident response teams must remain on high alert, ready to swiftly address cyber incidents, facilitate information sharing, and maintain active coordination with NCIIPC, CERT-In, and other regulatory bodies. All cyber incidents must be reported to NCIIPC at ir@nciipc.gov.in at the earliest, as well as to relevant exchanges and regulators, following the prescribed reporting mechanisms.
- Implement continuous monitoring of all privileged accounts to proactively detect and mitigate unauthorized access.
- Ensure that Managed Service Providers (MSPs) and vendors remain on a heightened state of alertness and strictly adhere to established cybersecurity best practices. Emphasize the deployment of high-quality personnel and the availability of standby response teams to swiftly address potential security incidents.
- Maintain strict monitoring of emails to detect and mitigate potential phishing attacks.
- Additionally, conduct continuous surveillance and timely reporting of phishing websites to prevent fraudulent activities and protect users from deceptive cyber threats.
- Ensure comprehensive protection of web-facing information infrastructure, including portals and websites, against Distributed Denial-of-Service (DDoS) attacks.

- Additionally, implement geo-fencing measures tailored to business requirements, restricting access based on geographic parameters to minimize exposure to potential threats while ensuring operational efficiency.
- Ensure employees are actively sensitized to cybersecurity threats, encouraging heightened awareness and proactive reporting of any phishing attempts, credential theft, or suspicious activities targeting organizational systems.
- Conduct continuous attack surface management, including regular Vulnerability Assessments (VA) of the network to identify and address security gaps.
- Ensure high availability of critical assets and services to maintain seamless business operations during unforeseen contingencies.
- Exercise caution in press and media interactions to prevent the unintended disclosure of tactical defense strategies and mitigate the risk of unnecessary panic.
- Establish clear communication guidelines, ensuring that sensitive security-related information remains protected while maintaining transparency and public confidence.

For and on behalf of
National Commodity & Derivatives Exchange Limited

Ravindra Shetty
Senior Vice President- Member Tech Compliance

For further information / clarifications, please contact

1. Customer Service Group on toll free number: 1800 26 62339
2. Customer Service Group by e-mail to : askus@ncdex.com