**NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED**

Circular to all members of the Exchange

Circular No. : NCDEX/Member Tech Compliance-007/2026

Date : April 13, 2026

Subject : Master Circular – Member Cyber Security related Compliance

1. This Master circular is a compilation of relevant circulars pertaining to "Cyber Security" issued by the Exchange which are operational as on date of this circular. Applicable provisions of existing circulars issued till March 31, 2026 are consolidated in this Master Circular.

2. It is hereby clarified that in case of any inconsistency between this Master Circular and the original applicable circular, the content of the original circular shall prevail.

3. Notwithstanding any revision in the processes or formats, if any -
   a) anything done or any action taken or purported to have been done or taken under such revised/ rescinded process including but not limited to any regulatory inspection/ investigation or enquiry commenced or any disciplinary proceeding initiated or to be initiated under such rescinded/ revised process or rescission, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular;
   b) the previous operation of the rescinded process or circular or anything duly done or suffered thereunder, any right, privilege, obligation or liability acquired, accrued or incurred thereunder, any penalty incurred in respect of any violation of such rescinded process or circulars, or any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability, penalty as aforesaid, shall remain unaffected as if the rescinded process or circulars have never been rescinded.

All Members, clients and market participants are requested to take note of the same.

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



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

**INDEX**





Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 1. Cyber security Incident reporting and Information sharing

**Background**

Cyber Incident Reporting is formal recording of facts related to cyber incidents occurred at the member end. Quarterly reports contain information on cyber-attacks and threats experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants. Members are required to submit the said information to Stock Exchanges / Depositories on quarterly basis as per the format prescribed in SEBI circular.

SEBI had issued a circular no. SEBI/HO/MIRSD/DOP/CIR/P/2019/109, dated October 15, 2019 prescribing format for quarterly reports containing information on cyber-attacks and threats experienced by Stock Broker and the timelines for submission of such reports. Accordingly, Exchange vide its circular no. NCDEX/TECHNOLOGY-065/2018 dated December 04, 2018 and circular no. NCDEX/RISK- 002/2019 dated October 18, 2019 had reiterated submission of duly filled quarterly report vide email on infosec@ncdex.com and on NSE Common Submission Portal within the prescribed timelines. The circular also prescribes qualification requirements for auditors and periodicity of audit of cyber security framework. Timelines are as given below:

| Sr. No. | Reporting Quarter in Financial Year | Reporting Quarter Dates | Due Date / Last Date for the submission of the report by the Member. |
|---|---|---|---|
| 1 | Q1 | 1 April to 30 June | 15th July |
| 2 | Q2 | 1 July to 30 September | 15th October |
| 3 | Q3 | 1 October to 31 December | 15 January |
| 4 | Q4 | 1 January to 31 March | 15th April |

Following are the relevant circulars issued by SEBI & the Exchange:

**SEBI Circular:**

- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024
- SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022
- SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022
- SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019
- SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

**Exchange Circular:**

- NCDEX/Member Tech Compliance-01/2026 dated January 06, 2026
- NCDEX/Member Tech Compliance-002/2025 dated January 09, 2025
- NCDEX/RISK- 006/2022 dated August 24, 2022
- NCDEX/RISK- 005/2022 dated July 01, 2022
- NCDEX/RISK- 002/2021 dated April 30, 2021
- NCDEX/RISK- 002/2020 dated September 22, 2020
- NCDEX/RISK- 002/2019 dated October 18, 2019
- NCDEX/RISK-001/2019 dated July 18, 2019
- NCDEX/TECHNOLOGY-065/2018 dated December 04, 2018



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 2. Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participant

**Background**

Cyber Security and Cyber Resilience audit report presents critical information about cybersecurity threats, risks within a digital ecosystem, gaps in security controls, and the performance of security programs highlighted by the auditor.

The Cyber Security and Cyber Resilience audit report is required to be submitted to the Exchange in digitally signed soft copy within the timelines indicated in circular by the member.

- **Type I Trading Members** – Annual Audit
- **Type II Trading Members** – Annual Audit
- **Type III Trading Members using NNF facility** – Half-yearly Audit
- **Type III Trading Members using Algo Trading and QSBs** – Half-yearly Audit

Submission of the Cyber Security and Cyber Resilience Audit Report shall be considered complete only upon submission along with management comments to the Exchange. The auditor shall indicate the compliance status for each ToR item as Compliant / Non-Compliant / Not Applicable, with justification for items marked as not applicable (refer Annexure A and B).

For each non-compliance reported by the auditor, Trading Members shall submit the Corrective Action Taken Report (ATR) within the prescribed timelines, based on which the auditor shall update the final compliance status on the ENIT portal.

Trading Members are advised to note Exchange Circular NCDEX/Member Tech Compliance-005/23 dated October 09, 2023 and Circular No. NCDEX/Member Tech Compliance-009/25 dated April 23, 2025, which specify the penalties, disciplinary actions, and charges for non-compliance (refer Annexure C).

The Audit Report shall be submitted in digitally signed soft copy within the stipulated timelines through the NSE common portal for NSE-registered members and via email to infosec@ncdex.com for NCDEX-registered members.

**Non/late submission of Cyber Security and Cyber Resilience Audit Report shall attract penal charges as mentioned in the Circular**.



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Following are the relevant circulars issued by SEBI & the Exchange:

**SEBI Circular:**

- SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022
- SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019
- SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

**Exchange Circular:**

- NCDEX/Member Tech Compliance-009/25 dated April 23, 2025
- NCDEX/Member Tech Compliance-009/24 dated October 14,2024
- NCDEX/Member Tech Compliance-003/2024 dated May 03, 2024
- NCDEX/Member Tech Compliance-002/2024 dated February 05, 2024
- NCDEX/Member Tech Compliance-007/23 dated October 27, 2023
- NCDEX/Member Tech Compliance-005/23 dated October 09, 2023
- NCDEX/RISK- 006/2023 dated May 18, 2023
- NCDEX/RISK- 007/2022 dated September 28, 2022
- NCDEX/RISK- 006/2022 dated 24, August 2022



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 3. Vulnerability Assessment and Penetration Testing (VAPT)

**Background**

VAPT stands for Vulnerability Assessment and Penetration Testing. It is the process of scanning for vulnerabilities and exploiting them to evaluate a system's security posture. VAPT gives a more detailed view of the threats that network or application is facing. It helps enterprises to protect their data and systems from malicious attacks. VAPT is important tool to accomplish compliance standards. VAPT protects the business from data loss arising out of unauthorized access.

Members needs to appoint external agency (CERT-In empaneled organizations) in order to conduct VAPT assignment.

With respect to the above provision, Stock Exchanges in consultation with SEBI, clarified that the VAPT shall be carried out and completed during the period September to November of every financial year and the final report on said VAPT shall be required to be submitted to the Stock Exchanges within one month from the date of completion of VAPT after approval from Technology Committee of respective Stock Brokers. In addition, Members should perform Vulnerability Assessment and Penetration Testing prior to the commissioning of a new system that is accessible over the internet.

Following are the relevant circular issued by SEBI & the Exchange:

**SEBI Circular:**

- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024
- SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

**Exchange Circular:**

- NCDEX/Member Tech Compliance-018/25 dated September 29, 2025
- NCDEX/Member Tech Compliance-007/24 dated September 16,2024
- NCDEX/Member Tech Compliance-004/23 dated September 22, 2023
- NCDEX/Member Tech Compliance-003/23 dated August 21, 2023
- NCDEX/RISK- 006/2022 dated August 24, 2022
- NCDEX/RISK- 003/2022 dated June 16, 2022
- NCDEX/TECHNOLOGY-065/2018 dated December 04, 2018



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

**4. Advisory for Financial Sector regarding Software as a Service based solutions**

**Background**

Software as a Service (SaaS) is also known as "On-Demand Software". It is a software distribution model in which a cloud service provider hosts services. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

Under guidance received from SEBI as per circular no. SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 dated November 03, 2020 & subsequent Amber advisory from CERT-In – 201155100308, Members have to confirm that whether specified confidential data and data types (as specified in the CERT-In advisory) are hosted/ not hosted on SaaS provider/ use or does not use any SaaS based GRC solutions on half yearly basis as per the prescribed format.

Following are the relevant circulars issued by SEBI & the Exchange:

**SEBI Circular:**

- SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 dated November 03, 2020

**Exchange Circular:**

- NCDEX/Member Tech Compliance-003/25 dated January 21, 2025
- NCDEX/Member Tech Compliance-006/24 dated July 18,2024
- NCDEX/Member Tech Compliance-001/2024 dated January 10, 2024
- NCDEX/Member Tech Compliance-001/2023 dated July 13, 2023
- NCDEX/RISK-001/2023 dated January 24, 2023
- NCDEX/RISK-008/2022 dated October 20, 2022
- NCDEX/RISK-004/2020 dated November 12, 2020



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 5. Framework to address the 'technical glitches' in Member's Electronic Trading Systems

**Background**

The Members of the Exchange are required, under various circulars and guidelines issued from time to time, to put in place adequate systems, processes, and controls to prevent system failures and ensure the provision of seamless trading services and facilities to their clients. As trading activities are increasingly conducted through electronic and technology-driven platforms, the resilience, reliability, and availability of Members' electronic trading systems have become critical to orderly market functioning and investor protection.

In order to address instances of technology-related disruptions at the Member level and to minimize their impact on clients and markets, a structured regulatory framework has been prescribed to identify, monitor, report, and manage technical glitches in Members' electronic trading systems. The framework also emphasizes the need for preventive and corrective measures through robust capacity planning, effective software testing and change management controls, and comprehensive Business Continuity Planning (BCP) and Disaster Recovery (DR) arrangements.

Accordingly, in consultation with the Securities and Exchange Board of India (SEBI) and other Stock Exchanges, it has been decided to issue detailed guidelines and a Standard Operating Procedure (SOP) to provide a uniform and systematic approach for handling technical glitches at the Member's end, along with a defined framework for Capacity Planning, Software Testing, Change Management, and BCP/DR preparedness. This SOP seeks to strengthen technology governance, enhance operational resilience, and ensure continued compliance with regulatory requirements while safeguarding the interests of investors.

- **Purpose-** This SOP sets out the framework, processes, and controls for the prevention, identification, reporting, investigation, and resolution of technical glitches in the Member's electronic trading systems to ensure uninterrupted trading services, regulatory compliance, market integrity, and investor protection.

- **Regulatory Reference.** - This SOP is framed in accordance with the SEBI Circular dated January 09, 2026 on Review of the Framework to Address Technical Glitches in Stock



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Brokers' Electronic Trading Systems and related guidelines issued by Stock Exchanges from time to time.

- **Definition of Technical Glitch-**A technical glitch shall mean any malfunction in the electronic system of the Member, including hardware, software, network or bandwidth, processes, products, or services, directly or indirectly related to trading and risk management, occurring during the trading session of a Stock Exchange, resulting in stoppage, slowdown, or variance in trading or risk management functions for a continuous period of five minutes or more.

- **Applicability**-This SOP shall apply to Members providing Internet-Based Trading (IBT) and/or Software Trading via Wireless Technology (STWT) platforms and having more than 10,000 registered clients, excluding closed accounts, as on 31st March of the previous financial year.

- **Reporting Requirements-**The Member shall intimate technical glitches to the Stock Exchange and clients within two hours of occurrence, submit a Preliminary Incident Report by T+1 day, and submit a Root Cause Analysis (RCA) report within 14 working days through the prescribed common reporting platform.

- **Capacity Planning**- Members shall undertake periodic capacity planning and monitor peak system loads to ensure continuity of services in accordance with Exchange guidelines.

- **Software Testing and Change Management**-All system changes shall be adequately tested before deployment, supported by documented testing and change management procedures.

- **Monitoring Mechanism**- Members' systems shall be subject to proactive monitoring, including Exchange-level monitoring through approved mechanisms.

- **Business Continuity and Disaster Recovery.**- Members shall maintain BCP and DRS arrangements as applicable, including defined RTO and RPO and periodic disaster recovery drills.



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

- **Effective Date**- This SOP shall come into effect from January 09, 2026 and supersedes previous instructions relating to technical glitches.

Following are the relevant circulars issued by SEBI & the Exchange:

**SEBI Circular:**

- SEBI/HO/ 38/44/12(1)2026-MIRSD-TPD1 dated January 09, 2026
- SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022

**Exchange Circular:**

- NCDEX/Member Tech Compliance-03/2026 dated January 12, 2026
- NCDEX/Member Tech Compliance-006/2025 dated March 28, 2025
- NCDEX/Member Tech Compliance-005/2025 dated January 30, 2025
- NCDEX/Member Tech Compliance/008-23 dated December 26, 2023
- NCDEX/Member Tech Compliance-002/2023 dated July 28, 2023
- NCDEX/RISK-004/2023 dated March 13, 2023
- NCDEX/RISK-010/2022 dated December 16, 2022
- NCDEX/RISK- 009/2022 dated December 05, 2022
- NCDEX/RISK- 005/2021 dated December 22, 2021



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 6. Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

**Background**

In recent times, the dependence on cloud computing for delivering the IT services is increasing. While cloud computing offers multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., the SEBI Regulated Entities (REs) are expected to be aware of the new cyber security risks and challenges which cloud computing introduces.

Following are the relevant circulars issued by SEBI & the Exchange:

**SEBI Circular:**

- SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023

**Exchange Circular:**

- NCDEX/RISK-003/2023 dated March 10, 2023



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 7. Advisory for Stockbroker – Member onboarding for CERT-In Cyber Swachhta Kendra (CSK)

**Background**

In recent times, there has been a surge in cyber-attacks in organizations across the globe impacting the continuity of their business operations and causing sensitive data leakage through malware infections at end point computing devices. To mitigate such malware and botnet infections, CERTIn has launched an initiative named 'Cyber Swachhta Kendra' (CSK) which provides information and enables organizations to disinfect the computing devices using free-of-cost malware and botnet cleaning tools.

In view of the above and to create a secure cyber eco-system, Stockbrokers providing Internet Based Trading platform and with more than 50,000 active traded clients are required to onboard themselves on 'Cyber Swachhta Kendra' Platform by November 06, 2023. Other members (not part of the above criteria) can also voluntarily subscribe to the services and avail actionable information intelligence from CSK.

For receiving the reports/alerts from Cyber Swachhta Kendra on daily basis, Stockbrokers are required to follow the certain procedure mention in the circular:

Following are the relevant circulars issued by the Exchange:

**Exchange Circular:**

- NCDEX/Member Tech Compliance-008/24 dated October 11, 2024
- NCDEX/Member Tech Compliance-006/23 dated on October 18, 2023



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 8. Advisory for Contribution of Information to RBI- FinTech Repository

**Background**

The EmTech repository portal is designed for the entities regulated by RBI such as banks and NBFCs, whereas the FinTech Repository aims to capture essential information of both regulated and unregulated entities. The purpose of the repository is to enhance understanding of the Indian FinTech sector from a regulatory perspective and facilitate the design of appropriate policy frameworks. The repositories being managed by the Reserve Bank Innovation Hub (RBIH), a wholly owned subsidiary of RBI, aims to provide aggregate sectoral data, trends, and analytics that will be beneficial for both policymakers and industry participants.

In this regard, SEBI has advised Exchanges to encourage their trading members to contribute information regarding the technological applications to FinTech Repository. The FinTech repository is accessible at the URL: https://fintechrepository.rbihub.in.

All Trading Members are advised to take note of the above advisory and requested to contribute information regarding the technological applications to FinTech Repository.

For further details on the repositories or assistance with submissions, trading members are requested to refer support details available on RBI hub/fintech website.

**Exchange Circular:**

- NCDEX/Member Tech Compliance-004/2025 dated on January 27, 2025



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

**9. Enhancement of API Authentication & Security for Exchange Empanelled Vendors (EV) and Application Service Providers (ASP's) and for trading members.**

**Background**

This is with reference to SEBI circular No.: SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018, and subsequent circulars regarding Cyber Security & Cyber Resilience framework for Stockbrokers. Securities Market organizations have been experiencing cyber-attacks which are rapidly growing in frequency and complexity.

Additionally, on analysis of these cyber-attacks reported by members in the past, it has been observed that these issues occurred due to vulnerable APIs used as part of the software products/services. To avoid occurrence of such cyber incidents and ensure secure usage of API, members are advised to adopt the following best practices.

&

Securities Market participants and entities have been experiencing cyber-attacks/incidents which are rapidly growing in frequency and complexity. In view of the recent cyber-attacks/incidents reported to Exchanges, it is observed that several instances of Cyber-attacks were due to exploitation of vulnerabilities found in Application Programming Interface (APIs) which is used for critical products/applications at members' end. These vulnerabilities could result in sensitive data leakage or may cause business disruption due to unauthorized access of these APIs by threat actors.

Considering the seriousness of these security incidents attributed to vulnerable APIs used as a part of the software products/applications, the Exchange empanelled software vendors and ASPs are required to follow the below mentioned best practices.

**Maintain Inventory of API**: Inventory of API including ownership, criticality/impact of API shall be maintained.

**Strong Authentication Mechanisms**: Employ strong & mutual authentication mechanisms such as API keys, OAuth, or IWT, ensuring secure token management practices and setting appropriate expiration times.

**Centralized API Security**: Establish an API gateway for centralized security enforcement and a web application firewall (WAF) to protect against common web threats. Implement an API security



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

gateway for both internal and external APIs. Disable any public API lacking secure authentication or strengthen it as per best practices at the earliest.

**Data Protection and Secure Communication**: Prioritize data protection by encrypting sensitive data, applying data masking techniques and using secure communication protocols to prevent eavesdropping and information leakage. Additionally, integrity checks through checksum or digital signature should be implemented to ensure data integrity & to avoid data manipulation/MITM.

**Input Validation and Output Encoding**: Validate and sanitize user inputs to prevent injection attacks and encode output to protect against HTML/JavaScript injection.

**Rate Limiting and Throttling**: Implement rate limiting and throttling mechanisms to prevent abuse and DDoS attacks, limiting requests from a single client within a specific time frame.

**Error Handling and Logging**: Ensure proper error handling and comprehensive logging for monitoring and auditing purposes.

**Cross-Origin Resource Sharing (CORS)**: Configure CORS properly to restrict unauthorized cross-origin requests.

**Secure Storage of Secrets**: Do not Store or Transmit API keys, credentials and sensitive data without secure encryption and access controls.

**Regular Security Assessments**: Conduct regular security assessments, including penetration testing, security audits, and code reviews. All APIs need to be assessed for security weakness/vulnerabilities and the checks should be aligned to OWASP Top 10 API security framework.

**Documentation**: Maintain clear documentation on secure API usage, including examples of proper authentication and authorization methods. For APIs facilitating sensitive business flows access shall be restricted on need-to-know basis.

**Privacy Protection:** Minimize data collection to essential information, comply with relevant privacy regulations and obtain user consent for data processing. Integrate privacy considerations from the initial stages of API development, performing a Privacy Impact Assessment (PIA) to identify and mitigate potential privacy risks.



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

**Secure Software Development Lifecycle (SDLC):** Integrate security considerations into the entire API development process and conduct security training for developers to promote secure coding practices.

**Annual Software Audit (ISO 12207:2017)**: Conduct an annual software assessment as per ISO 12207:2017 standards for Systems and Software Engineering.

All Exchange Empaneled vendors/ASPs are required to comply with the above best practices.

**SEBI Circular:**

- SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018

**Exchange Circular:**

- NCDEX/Member Tech Compliance-004/24 dated on July 12, 2024
- NCDEX/Member Tech Compliance-005/24 dated om July 12, 2024



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 10.Advisory on Cyber Security Preparedness for current Geo-Political Development

**Background**

In view of the current Geo-political developments, the possibility of state and non-state actors targeting the financial market seems higher than usual. In such circumstances, it is important to maintain a high level of readiness for any such cyber incidents.

Members are requested to take steps to:

- Implement necessary measures for enhancing security of Internet facing applications and websites.
- Ensure that all devices are integrated and being monitored by Security Operations Center (SOC).
- Strengthen effectiveness of existing security controls and incident management plan
- Review and action all advisories/alerts received from CERT-In/ NCIIPC on priority.
- Be on high alert and monitor any suspicious traffic / activity.
- Monitor all network traffic from within and outside network to identify DDoS or Ransomware attacks, defacing or disrupting digital infrastructure, breaching of the confidentiality, integrity and availability through various attack vectors etc.
- Conduct Vulnerability assessment and mitigate findings in a timely manner.
- Timely report incidents/anomalies to Exchanges & Regulators as per defined reporting mechanism.

**Exchange Circular:**

- NCDEX/Member Tech Compliance-010/2025 dated May 09, 2025



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 11. Implementation of Two-Factor Authentication for Client logins on Stockbrokers offering IBT & STWT platforms

**Background**

This has reference to the Exchange Circular no NCDEX/RISK- 004/2022 dated June 16, 2022, regarding the implementation of Two-Factor Authentication (2FA).

In accordance with the aforementioned Exchange circular, all Members were mandated to implement Two-Factor Authentication for client login on applications offered through Internet-Based Trading (IBT) and Securities Trading through Wireless Technology (STWT) platforms.

In continuation to the above and considering the risk associated with cyber security and cyber threats, it is hereby reiterated that trading members shall ensure the implementation of Two-Factor Authentication for each login attempt, whether through mobile (STWT) or web-based trading applications (IBT).

In the recent past it has been observed that the client/investor log-in session remained active covering multiple trading session/days irrespective of trading/non-trading activity by client/investor. Accordingly, it is advised that active log-in session through IBT & STWT platforms be logged-out at the time of End of-Day processing (EOD)/at defined time and subsequent login by clients/investors should only be permitted after successful Two-Factor Authentication (2FA).

**Exchange Circular:**

- NCDEX/Member Tech Compliance-012/2025 dated June 19, 2025



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

## 12. Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) . for SEBI Regulated Entities(REs)

**Background**

This is with reference to SEBI Circular No. SEBI/HO/ITD 1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, on 'Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) and subsequent clarification circulars dated December 31, 2024, March 28, 2025, April 30, 2025, August 28, 2025, and Frequently Asked Questions (FAQ) dated June 11, 2025 issued by SEBI.

For the implementation of CSCRF guidelines by REs, following has been clarified in consultation with SEBI:

1. For determining the Number of total registered clients (as provided in Clause 2.1.1, Table 1 (Page No 2) of the SEBI Circular No. SEBI/HO/ ITD 1/ITD_CSC_EXT/P/CIR/2025/60 dated April 30, 2025), it shall include "Number of clients with status reported as active and inactive based on Unique PAN, excluding the clients which are marked/reported as Closed by the stockbroker's/trading members. Accordingly, the parameter shall be read as Registered Clients based on Unique PAN, which shall include status reported as Active & Inactive by trading Members and clients for which status has been reported as Closed in UCC database shall not be considered.

2.In case trading member/RE is engaged in clientele as well as proprietary trading (as specified in point no 6.2 of SEBI Frequently Asked Questions (FAQs) dated June 11, 2025 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs), for such trading members/REs, if the clientele trading turnover is less than 10% of their proprietary trading turnover during the financial year period April 1 to March 31, such trading members/REs shall be categorized/considered as proprietary stockbrokers/trading members for the purpose of applicability of CSCRF.**SEBI Circular:**

- SEBI/HO/ITD 1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024

**Exchange Circular:**

- NCDEX/Member Tech Compliance-015/25 dated September 2, 2025



Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com