NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to all members of the Exchange

Circular No. : NCDEX/RISK-008/2023

Date : June 30, 2023

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 May 30, 2023 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   a) anything done or any action taken or purported to have been done or taken under such revised/ rescinded process including but not limited to any regulatory inspection/ investigation or enquiry commenced or any disciplinary proceeding initiated or to be initiated under such rescinded/ revised process or rescission, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular;

   b) the previous operation of the rescinded process or circular or anything duly done or suffered thereunder, any right, privilege, obligation or liability acquired, accrued or incurred thereunder, any penalty incurred in respect of any violation of such rescinded process or circulars, or any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability, penalty as aforesaid, shall remain unaffected as if the rescinded process or circulars have never been rescinded.

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

For and on behalf of
National Commodity & Derivatives Exchange Limited

Sanjay Jain
Senior Vice President and CISO – Enterprise Risk and Governance

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" 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/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

Exchange Circular:

- 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

Exchange vide its circular no. NCDEX/TECHNOLOGY-065/2018 dated December 4, 2018 had included copy of SEBI circular no. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, which contained following:

- **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. Members using CTCL/IBT/STWT facility/ Members trading through the Exchange provided Traded Work Solution (TWS) – Type of Broker – I / II are required to submit reports on yearly basis. Further, all the members using ATF Facility – Type of Broker – III, are required to conduct audit on half-yearly basis.

The guidelines annexed was effective from April 1, 2019.

- The members are advised to submit the following documents in a digitally signed soft copy in PDF format to the Exchange:

1. Cyber Security and Cyber Resilience Audit Report (**Annexure A**) along with Executive summary (**Annexure B**).

   Download Link Annexure A & B – https://ncdex.com/quick_links/download

2. Action Taken Report, if applicable.

3. Follow-on report with management comments if applicable (Annexure C), as per the time line provided.

Non/late submission of Cyber Security and Cyber Resilience Audit Report shall attract penal charges as mentioned below.

- Penalty of Rs. 200/- per day on members failing to submit the said reports within 1 month from the end of due date of submission,
- Penalty of Rs. 500/- per day after 1 month but within 3 months from the end of the due date for submission and
- Disablement of trading facility across segments after giving 2 weeks' notice for non-submission within 3 months from the end of due date for submission.

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/DOP/CIR/P/2019/109 dated October 15, 2019
- SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Exchange Circular:

- NCDEX/RISK- 006/2023 dated May 18, 2023
- NCDEX/RISK- 007/2022 dated September 28, 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/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Exchange Circular:

- 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/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, through various circulars, and guidelines, issued from time to time, have been required to put in place various measures / controls, to prevent system failures and to ensure the provision of seamless service / facilities to their clients. In furtherance to the above, in consultation with SEBI and other Exchanges, it has been decided to issue guidelines / Standard Operating Procedure (SOP) for handling technical glitches at the Members end as well as provide a framework for Capacity Planning, Software Testing, Change management and Business Continuity Planning (BCP) / Disaster Recovery (DR).

The top 20 Members registered with the Exchange, having the most Internet and Wireless technology based (IBT/STWT) clients are classified as 'Specified Members' for this purpose. In adherence to the above and in consultation with other Exchanges, 35 Members have been identified as 'Specified Members'.

In specific, points 3.viii, 4.vi, 5.i, 5.ii, 5.iii, 6.v, 6.xiii, 6.xiv are only applicable to 'Specified Members', over and above the other points as stated in 'Annexure-A' of the circular no. NCDEX/RISK-010/2022 dated December 16, 2022.

Technical Glitches:

'Technical glitch' shall mean any malfunction in the Member's systems including malfunction in its hardware, software, networks, processes, or any products or services provided by the Member in the electronic form. The malfunction can be on account of inadequate Infrastructure/systems, cyberattacks/incidents, procedural errors, and omissions, or process failures or otherwise, in their own systems or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the normal functions/operations/services of systems of the Member for a contiguous period of five minutes (5 minutes) or more.

'Critical Systems' are defined as all IT systems that are related to Trading applications and trading-related services.

All Members shall be required to report to the Exchange any technical glitches as under:

i. All Members shall inform about the technical glitch to the stock exchanges immediately but not later than 1 hour from the time of occurrence of the glitch.

ii. Members shall submit a Preliminary Incident Report to the Exchange within T+1 day of the incident ('T' being the date of the incident). The report shall include the date and time of the incident, details of the incident, effect of the incident, and immediate action taken to rectify the problem.

iii. Members shall submit a Root Cause Analysis (RCA) Report of the technical glitch to the stock exchange, within 14 days from the date of the incident. The RCA report, for all technical glitch incidents greater than 45 minutes, shall also be verified by an independent auditor appointed by the Member.

Submission of all the above three reports shall be as per the format provided in 'Annexure-B' of the SEBI 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

The members reporting the incident pertaining to technical glitch should send aforementioned documents via email to the specified email id - infotechglitch@nse.co.in . Members should submit the documents as specified.

Capacity Planning:

i. Increasing number of investors may create an additional burden on the trading system of Members and hence, adequate capacity planning is a prerequisite for Members to provide continuity of services to their clients.

ii. Members shall do capacity planning for the 'Critical Systems' infrastructure including server capacities, network availability, and the serving capacity of trading applications.

iii. Capacity planning shall be done based on the rate of growth in the number of transactions observed in the past 2 years. This data should be extrapolated to predict the capacity required for the next 3 years.

Software testing and change management:

i. Software applications are prone to updates/changes and hence, it is imperative for the Members to ensure that all software changes that are taking place in their applications are rigorously tested before they are used in production systems. Software changes could impact the functioning of the software if adequate testing is not carried out. In view of this, Members shall adopt the following framework for carrying out software-related changes/testing in their systems.

ii. Members shall create test-driven environments for all types of software developed by them or their vendors.

Monitoring mechanism – Applicable to 'Specified Members'

i. Proactively and independently monitoring technical glitches shall be one of the approaches in mitigating the impact of such glitches. In this context, the 'Specified Members' shall build API-based Logging and Monitoring Mechanism (LAMA) to allow stock exchanges to monitor the 'Key Parameters' of the 'Critical Systems'. Under this mechanism, 'Specified Members' shall monitor key systems & functional parameters to ensure that their trading systems function in a smooth manner. Stock exchanges will, through the API gateway, independently monitor these key parameters in real-time to gauge the health of the 'Critical Systems' of the 'Specified Members'.

ii. The 'Specified Members' and the Exchange will preserve the logs of the key parameters for a period of 30 days in the normal course. However, if a technical glitch takes place, the data related to the glitch shall be maintained for a period of 2 years.

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

Business Continuity Planning (BCP) and Disaster Recovery Site (DRS):

i. 'Specified Members' and Members with a minimum client base of 50,000 clients across all Exchanges, are to mandatorily establish a 'Business Continuity'/ 'Disaster Recovery setup'.

ii. Members shall put in place a comprehensive BCP-DR policy document outlining standard operating procedures to be followed in the event of any 'Disaster'.

iii. 'Disaster' may be defined as scenarios where:

a. A 45-minute disruption of any of the 'Critical Systems', or
b. Any additional criteria specified by the Governing Board of the Member.

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

SEBI Circular:

- SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022

Exchange Circular:

- 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. Cyber Security Advisories issued by SEBI / CERT-In / NCIIPC & Exchange.

• Background

In view of the rising incidents of data breaches / data leaks / cyber-attacks etc. SEBI / CERT–In / NCIIPC issued Cyber Security guidelines. All members were advised to adhere the Cyber Security guidelines / advisories issued and also comply with the guidelines issued by SEBI / CERT-In and NCIIPC from time to time.

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

SEBI Circular:

- SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023
- SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Exchange Circular:

- NCDEX/RISK- 002/2023 dated February 24, 2023
- NCDEX/RISK- 001/2022 dated March 3, 2022
- NCDEX/RISK- 004/2021 dated November 26, 2021
- NCDEX/RISK- 002/2021 dated April 30, 2021
- NCDEX/RISK- 001/2020 dated April 15, 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

7. 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

8. Implementation of Two Factor Authentication

- **Background**

Members were required to mandatorily implement two-factor authentication on application offered by Members to customers through Internet Based Trading (IBT) and Securities Trading using Wireless Technology (STWT).

In joint consultation with SEBI and Exchanges, it was clarified that, in addition to user ID, Members shall preferably use biometric authentication as one of the authentication factors, along with any one of the below-mentioned factors:

1. Knowledge factor (something only the user knows): - for e.g., Password, PIN
2. Possession factor (something only the user has): - for e.g., OTP, security token, authenticator apps on smartphones etc. In case of OTP, the same should be sent to clients through both email and SMS on their registered email ID and Mobile number.

In cases, where biometric authentication is not possible, Members shall use both the aforementioned factors (Knowledge factor and Possession factor), in addition to the user ID, for 2- factor authentication (2FA). It is to be noted that the above-mentioned authentication shall be implemented on every login session by the client to IBT and STWT.

Following is the relevant circular issued by the Exchange:

Exchange Circular:

- NCDEX/RISK-004/2022 dated June 16, 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