NCDEX
Pragati ka Solid Exchange

NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to all members of the Exchange

Circular No. : NCDEX/Member Tech Compliance-009/25

Date : April 23, 2025

Subject : Cyber Security and Cyber Resilience Audit of Trading Members

This is with reference to the SEBI circular no. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019, SEBI/HO/MIRSD /TPD/P/CIR/2022/80 dated June 07, 2022, SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 and Exchange circular no. NCDEX/TECHNOLOGY-065/2018 dated December 4, 2018, NCDEX/TECHNOLOGY011/2019 dated March 25, 2019, NCDEX/RISK- 002/2019 dated October 18, 2019, NCDEX/RISK- 003/2022 dated 16, June 2022, NCDEX/RISK- 006/2022 dated 24, August 2022, in relation to Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participant, trading members are required to conduct Cyber Security and Cyber Resilience audit and submit the report to the Exchange.

Reference is further drawn to para 5 of the said SEBI Circular dated October 15, 2019, wherein periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience is defined. Accordingly, trading members are required to carry out an audit for the period ended March 31, 2025, as per the applicability criteria given below:

Category of Member	**Type I**	**Type II Using NNF**	**Type III Using Algo & QSB**
Trading Members	Annually	Annually	Half Yearly

The timelines for submissions of the Audit report are given below:

Audit Period	**Due date for submission for QSB and Non-QSB Members**	
	Preliminary Audit Report submission	**Corrective Action taken Report (ATR) submission.** **(If applicable)**
Half Yearly (October 2024 - March 2025)	June 30, 2025	September 30, 2025
Yearly Submission (April 2024 - March 2025)	June 30, 2025	September 30, 2025

Submission of Cyber Security and Cyber Resilience Audit Report shall be considered complete only after the trading member submits the report to the Exchange after providing management comments. Further, the auditor must provide compliance status for each TOR item as Compliant/Non-Compliant/Not Applicable and in case of any TOR item which is not applicable, auditor is required to provide justification for non-applicability of said TOR. The guidelines on auditor selection norms has been given in Annexure A and the detailed ToR applicable for Cyber Audit has been given in Annexure B.

All Trading members are requested to take note that, for each non-compliance reported by the auditor, trading members are required to submit corrective action taken report as per the above-mentioned timelines. On review of details of corrective action submitted by trading members, the auditor shall submit the status of compliance as Compliant or Non-Compliant on ENIT.

Trading Members are requested to take note of the Exchange circular NCDEX/Member Tech Compliance-005/23 dated October 09, 2023, regarding penalties/disciplinary action(s)/charges for Cyber Security and Cyber Resilience Audit Report related submissions, the details of the same have been provided in Annexure C.

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 below. The said reports are to be sent as an attachment only to email ID: infosec@ncdex.com.

All Trading Members are advised to take note of the above and comply.

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

Annexure A

Auditor Selection Norms

1. The Audit shall be conducted by **CERT-In empaneled organization/entity.**

2. The Auditor/Auditor firm can perform a maximum of 3 successive audits of the Trading Members. However, such an auditor shall be eligible for reappointment after a cooling – off period of one year.

3. The Auditor, as being appointed by Trading Member must not have any conflict of interest in conducting fair, objective, and independent audit. Further, the directors / partners of Audit firm shall not be related to any Directors/Promoters/Proprietor of the said Trading Members either directly or indirectly.

4. The Auditor should not have been engaged over the last three years in any consulting engagement with any departments / units of the Trading Member.

5. The Auditor shall not have any cases pending against its previous audited companies/firms, which fall under SEBI’s jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

6. The trading members and auditors are required to retain records of physical visits conducted during audits like name, qualification & date of visit/s of auditor, along with audit artifacts, proofs of concept (POCs), and evidence related to terms of reference (TOR) points for a minimum duration of three years. At time of auditor registration, trading members are requested to provide & upload details of auditor appointment and auditor qualification certificate.

Annexure B

Terms of Reference (TOR) for Cyber Security Audit Report.

Audit TOR Clause	Details
1	**Governance**
1(a)(i)	Whether the Stockbroker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular?
1(a)(ii)	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document?
1(a)(iii)	Is the policy document approved by the Board / Partners / Proprietor of the organization?
1(a)(iv)	Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
1(a)(v)	Policy Approval Date
1(a)(vi)	Policy Version
1(a)(vii)	Policy Approval By
1(b)(i)	Whether the Cyber Security Policy includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks, and systems:
1(b)(ii)	a. 'Identify' critical IT assets and risks associated with such assets.
1(b)(iii)	b. 'Protect' assets by deploying suitable controls, tools, and measures.
1(b)(iv)	c. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes.
1(b)(v)	d. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack.
1(b)(vi)	e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
1(c)	Whether policy / Procedure document refers to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
1(d)	Whether policy document have considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.
1(e)	Stockbrokers / Depository Participants should designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the

	establishment and implementation of processes and procedures as per the Cyber Security Policy.
1(f)(i)	Whether the Member has constituted a Technology Committee comprising experts.
1(f)(ii)	This Technology Committee has reviewed on a half yearly basis the implementation of the Cyber Security and Cyber Resilience policy, which includes:
1(f)(iii)	- review of their current IT and Cyber Security and Cyber Resilience capabilities,
1(f)(iv)	- if committee has set goals for a target level of Cyber Resilience and establish plans to improve and strengthen Cyber Security and Cyber Resilience.
1(f)(v)	- And the review report is placed before the Board / Partners / Proprietor of the Stockbrokers / Depository Participants for appropriate action.
1(g)	Whether the Designated officer and the technology committee periodically reviewed instances of cyber-attacks, if any, domestically and globally, and taken steps to strengthen Cyber Security and cyber resilience framework.
1(h)	Whether Brokers / Depository Participants has policy or reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
1(i)	Has Stockbroker/Depository Participant defined and documented roles and responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Stockbroker/Depository Participants towards ensuring the goal of Cyber Security?
1(j)	Stockbrokers / Depository Participants should prepare detailed incident response plan and define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)
2	**Identification**
2(a)	Has the Stockbroker / Depository Participant identified and classified critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board/Partners/Proprietor of the Stockbrokers / Depository Participants shall approve the list of critical systems **at least on half yearly basis**. To this end, Stockbrokers / Depository Participants should maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

2(b)	Has the Stockbrokers / Depository Participants identified / has process to identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
3	**Protection**
3(a)	Access control No person by virtue of rank or position should have any intrinsic right to access Confidential data, applications, system resources or facilities.
3(b)	Access control Any and all access to Stockbrokers / Depository Participants systems, applications, networks, databases etc., have defined purpose and for a defined period. Stockbrokers / Depository Participants should grant access to IT systems **(servers, network devices, endpoints etc.)**, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege to provide security for both on-and off-premises resources (i.e. zero-trust models). This security models requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter. Such access should be for the period when the access is required and should be authorized using multi factor authentication (MFA). Maker and Checker framework should be implemented in strict manner and enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and user accounts that access critical systems and applications.
3(c)	Have Stockbrokers / Depository Participants implemented an access policy which addresses strong password controls for users' access to systems, applications, networks, and databases. The policy should include a clause of: 1. Periodic review of accounts of ex-employees. 2. Passwords should not be reused across multiple accounts. 3. List of passwords should not be stored on the system. Illustrative examples for strong password controls are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3(d)	All critical systems of the Stockbroker / Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
3(e)	Stockbrokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a period not less than two (2) years. Stockbrokers / Depository Participants should implement strong log retention policy as per extant SEBI regulations and required by CERT-In and IT Act 2000. Stockbrokers / Depository Participants are advised to audit that all logs that are being collected. Stockbrokers / Depository Participants should monitor incidents to identify unusual patterns and behaviours.

3(f)	Stockbrokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stockbroker / Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, Maker-Checker framework should be implemented for modifying the user's right in internal applications, etc.
3(g)	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stockbrokers / Depository Participants critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
3(h)	Stockbrokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Stockbroker / Depository Participant's critical IT infrastructure.
3(i)	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
4	**Physical Security**
4(a)	Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied by authorized employees.
4(b)	Physical access to the critical systems should be revoked immediately if the same is no longer required.
4(c)	Stockbrokers/ Depository Participants has ensured that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human, and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate
5	**Network Security Management**
5(a)	Stockbrokers / Depository Participants has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment.
5(b)	The LAN and wireless networks should be secured within the Stockbrokers /Depository Participants' premises with proper access controls.
5(c)	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.
5(d)	Stockbrokers / Depository Participants should install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
5(e)	Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application-based IDS systems, customized kernels for Linux, anti-virus, and anti-malware software etc.

5(f)	Stockbrokers / Depository Participants should deploy web and email filters on the network. Stockbrokers / Depository Participants should configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. **A reputable antivirus solution should be deployed across all endpoints and wherever possible on servers.** Stockbrokers / Depository Participants should scan all emails, attachments, and downloads both on the host and at the mail gateway **using the antivirus solution.**
5(g)	Stockbrokers / Depository Participants should block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
5(h)	Stockbrokers / Depository Participants should restrict execution of **"Command Prompt"**, “PowerShell” and “wscript” in enterprise environment, if not required. **In case of requirement, the Stockbrokers / Depository Participants should maintain appropriate business approval and should limit the same to authorised personnel only for the time required.** Stockbrokers / Depository Participants should ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Stockbrokers / Depository Participants should send the associated logs to a centralized log repository for monitoring and analysis.
5(i)	Stockbrokers / Depository Participants should utilize host-based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
5(j)	Stockbrokers / Depository Participants should implement practice of whitelisting of ports based on business usage at Firewall level rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.
5(k)	Is Network Time Protocol (NTP) server configured to synchronise with National Physical Laboratory (NPL) or National Informatics Centre (NIC) or any associated servers for synchronisation of all ICT system clocks?
6	**Data security**
6(a)	Critical/sensitive and Personally Identifiable Information (PII) data must be identified, classified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6(b)	Stockbrokers / Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6(c)	The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that

	can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
6(d)	Stockbrokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
6(e)	Stockbrokers / Depository Participants should Enforce BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection
6(f)	Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create data leakage prevention (DLP) solutions / processes inclusive of detection, alerting, prevention, containment & response to a data breach/ data leak. **Is the DLP configured/ deployed across all the endpoints (end users), email and network? Are relevant policies/ rules configured on the DLP to prevent exfiltration of PII data, sensitive and confidential data from within the organisation and organisational assets? Does the DLP solution / process support alerting / blocking of movement of data from within the organisation to an unauthorised external domain?**
6(g)	Stockbrokers/ Depository Participants shall enforce effective data protection, backup, and recovery measures.
7	**Hardening of Hardware and Software**
7(a)	Whether Member only deploys hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
7(b)	Whether Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.
8	**Application Security in Customer Facing Applications**
8(a)	Whether over the Internet application like IBTs (Internet Based Trading applications) portal and back-office application, containing sensitive or private information are secured by using security measures. (Illustrative list of measures for ensuring security in such applications is provided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
9	**Certification of off-the-shelf products**
9(a)	Stockbrokers / Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back-office applications) should 1. bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). or 2. Certified independently on criteria similar to Indian Common Criteria Certificate of Evaluation Assurance Level. Custom developed / in-house software and components need not obtain the certification, but must undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.

10	**Patch management**
10(a)	Stockbrokers / Depository Participants should include All operating systems and applications for updating latest patches on a regular basis. Stockbrokers / Depository Participants should establish and ensure that the patch management procedures including the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner. As an interim measure for zero-day vulnerabilities and where patches are not available, Stockbrokers / Depository Participants can consider virtual patching for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
10(b)	Stockbrokers / Depository Participants should perform rigorous testing of security patches and updates **in UAT environment**, where possible, before deployment into the production environment to ensure that the application of patches does not impact other systems.
11	**Disposal of data, systems, and storage devices**
11(a)	Stockbrokers / Depository Participants should frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.
11(b)	Stockbrokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
12	**Vulnerability Assessment and Penetration Testing (VAPT)**
12(a)	Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include all critical assets **(as per the recently updated and approved critical asset list including newly commissioned assets, if any)** and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system.
12(b)	Stockbrokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stockbrokers / Depository Participants are required to engage only CERT-In empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stockbrokers / Depository Participants, within 1 month of completion of VAPT activity.
12(c)	In addition, Stockbrokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
12(d)	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, Stockbrokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.

12(e)	Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report.
13	**Monitoring and Detection**
13(a)	Stockbrokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies to identify unusual patterns and behaviours.
13(b)	Further, to ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet, Stockbrokers / Depository Participants should implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
13(c)	Stockbrokers / Depository Participants should proactively monitor the cyberspace to identify phishing websites w.r.t. to REs/Member domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
14	**Response and Recovery**
14(a)	Alerts generated from monitoring and detection systems should be suitably investigated to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect, and eradicate the incident.
14(b)	The response and recovery plan of the Stockbrokers / Depository Participants should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stockbrokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012, as amended from time to time
14(c)	The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.
14(d)	Any incident of loss or destruction of data or systems should be thoroughly analysed
14(e)	And lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
14(f)	Stockbrokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan. Whether the stockbroker has conducted Periodic DR drills in accordance with Exchange Circular NSE/COMP/54876 dated December 16, 2022?
15	**Sharing of Information**

15(a)	All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stockbrokers / Depositories Participants shall be reported to Stock Exchanges / Depositories /CERT-IN & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: incident@cert-in.org.in, **mkt_incidents@sebi.gov.in and group email ID of all MIIs - member.cir@bseindia.com.**
15(b)	The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stockbrokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
15(c)	The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches 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 / Exchanges /Depositories and SEBI, shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.
16	**Training and Education**
16(a)	Stockbrokers / Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).
16(b)	Stockbrokers / Depository Participants should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts and advisories issued by CERT-In/ CSIRT-Fin that may be referred for assistance in conducting exercises for public awareness. Where possible, this should be extended to outsourced staff, vendors etc. The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.
16(c)	Stockbrokers / Depository Participants should Provide training to the employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they should not use their corporate device- especially in Work from Home environments.
17	**Systems managed by vendors**
17(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.
18	**SEBI and Exchange Compliances**

18(a)	Auditor to list all applicable implementation of Circulars, Notices, Guidelines, and advisories published by CERT-In/ CSIRT-Fin Advisories, SEBI and Exchanges.
18(b)	1- Adherence to all such Circulars, Notices, Guidelines, and advisories published
18(c)	2- Reporting adherences based on prescribed periodicity in point 1 above
19	**Advisory for Financial Sector Organizations:**
19(a)	Whether compliance of the SEBI circular no. SEBI/HO/MIRSD2/DOR/CIR/P/ 2020/221 dated November 03, 2020, for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made.
20	**Cyber Security Advisory - Standard Operating Procedure (SOP)**
20(a)	Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether stockbroker has to be complied. **Please refer Exchange circular reference no. NSE/INSP/66040 dated January 08, 2025.**
20(b)	**Members shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure-SOP) in place. Such policy shall be approved by Internal Technology Committee of the member, as the case may be and shall be reviewed at least annually. The Cyber Security Incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.** **Please refer Exchange circular no. NSE/INSP/66040 dated January 08,2025.**
20(c)	Members shall examine the Cyber Security incident and classify the Cyber Security incidents into **Critical**/High/ Medium/ Low as per their Cyber Security incident handling process document. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.
20(d)	Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In).
20(e)	**Any cyber-attack(s), cybersecurity incident(s) and breach(es) experienced by member as per the threshold for classifying incidents shall be notified to SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the email ID mkt_incidents@sebi.gov.in and group email ID of all MIIs- member.cir@bseindia.com within 6 hours and SEBI Incident Reporting Portal within 24 hours. Trading member/ Depository Participants shall also report the incident(s) to Stock Exchanges/ Depositories along with SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents.**
20(f)	Members shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, details need to be provided to Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.

20(g)	The details of the reported Cyber Security incident and submission to various agencies by the Members shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of **SEC-MIRSD, TPD-MIRSD** and CISO of SEBI.
20(h)	The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned **SEBI Circular no. SEBI/HO/MIRSD/CIR/PB/2018/147** dated December 03, 2018) shall continue to report any unusual activities and events within 6 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter in the manner as specified in Exchange circular.
21	**Security of Cloud Services:**
21(a)	Stockbrokers / Depository Participants should check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
21(b)	Stockbrokers / Depository Participants should ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.
21(c)	Stockbrokers / Depository Participants should implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.
21(d)	Stockbrokers / Depository Participants should consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
21(e)	Governance, Risk and Compliance (GRC) Ensure alignment with Governance, Risk, and Compliance (GRC) standards within cloud computing operations and practices. Refer principle 1 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(f)	Selection of Cloud Service Providers Ensure compliance with established guidelines and protocols in the selection and engagement of cloud service providers. Refer principle 2 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(g)	Data Ownership and Data Localization Ensure compliance with data ownership and localization requirements as mandated by relevant regulations and policies within cloud operations. Refer principle 3 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(h)	Responsibility of the Regulated Entity Ensure that the Regulated Entity assumes responsibility for maintaining compliance with all relevant cloud computing regulations and standards. Refer principle 4 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023

21(i)	Due Diligence by the Regulated Entity Ensure that the Regulated Entity conducts thorough due diligence when assessing cloud service providers and their compliance with regulatory requirements. Refer principle 5 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(j)	Security Controls Implement and maintain robust security controls to safeguard data and systems in compliance with cloud computing regulations and standards. Refer principle 6 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(k)	Contractual and Regulatory Obligations Ensure that contractual agreements with cloud service providers align with regulatory obligations to maintain compliance within cloud operations. Refer principle 7 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(l)	BCP, Disaster Recovery & Cyber Resilience Integrate Business Continuity Planning (BCP), Disaster Recovery, and Cyber Resilience measures into cloud operations to ensure compliance with regulatory requirements. Refer principle 8 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
21(m)	Vendor Lock-In and Concentration Risk Management Implement strategies to manage vendor lock-in and concentration risks effectively in cloud operations to maintain compliance with regulatory standards. Refer principle 9 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22	**Concentration Risk on Outsourced Agencies:**
22(a)	Stockbrokers / Depository Participants should take into account concentration risk (Single third-party vendors are providing services to multiple Stockbrokers / Depository Participants) while outsourcing multiple critical services to the same vendor.
23	**API Authentication & Security:**
23 (a)	Stockbrokers / Depository Participants should ensure maintain inventory of API with details including ownership, criticality/impact, **type (external/ internal) of API, etc.** shall be maintained.
23 (b)	Stockbrokers / Depository Participants should ensure Strong Authentication Mechanisms which should ensure strong & mutual authentication mechanisms such as API keys, OAuth, or IWT, ensuring secure token management practices and setting appropriate **expiration times should be defined.**
23 (c)	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 gateway for both internal and external APIs. Disable any public API lacking secure authentication or strengthen it as per advisory at the earliest. Please refer NSE Circular ref. no. NSE/MSD/62913 dated July 11, 2024.

23 (d)	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
23 (e)	Input Validation and Output Encoding: Validate and sanitize user inputs to prevent injection attacks and encode output to protect against HTML/JavaScript injection.
23 (f)	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.
23 (g)	Error Handling and Logging: Ensure proper error handling and comprehensive logging for monitoring and auditing purposes.
23 (h)	Cross-Origin Resource Sharing (CORS): Configure CORS properly to restrict unauthorized cross-origin requests.
23 (i)	Secure Storage of Secrets: Do not Store or Transmit API keys, credentials and sensitive data without secure encryption and access controls.
23 (j)	Regular Security Assessments: Conduct regular security assessments, including penetration testing, security audits, and code reviews. All API's need to be assessed for security weakness/vulnerabilities and the checks should be aligned to OWASP Top 10 API security framework.
23 (k)	Documentation: Maintain clear documentation on secure API usage, including examples of proper authentication and authorization methods. For API's facilitating sensitive business flows access shall be restricted on need-to-know basis.
23 (l)	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.
23 (m)	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.

Annexure C

Penalty/disciplinary action for Delay/Non-submission of Preliminary Audit Report / Corrective Action Taken Report and non-Closure of observations.

The following penalty/disciplinary actions as provided in Table A would be initiated against the Trading Member for Delay/Non-submission of Preliminary Audit Report and Corrective Action Taken Report.

Table – A

Details of Violation	**Period of violation**	**Penalty/disciplinary actions**	**Penalty/disciplinaryaction in case of repeated violation**
Delay /Non-Submission of Preliminary audit /Corrective Action Taken Report	From 1st day to 7th day:	Charges Rs. 1,500/- per day for Non QSB & Rs. 3,000/- per day for QSB from the due date till first 7 calendar days or submission of report, whichever is earlier.	In case of a repeat instance by the Trading Member, levy of applicable monetary penalty along with an escalation of 50%.
	From 8th day to 21st day:	Charges of Rs. 2,500/- per day for Non QSB & Rs. 5,000/- per day for QSB from 8th calendar day after the due date to 21st calendar day or submission of report, whichever is earlier.	Levy of applicable monetary penalty along with an escalation of 50%.
	From 22nd day onwards:	In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. The disablement notice issued to the Trading Member will be shared with all the Exchanges for information.	
	After 28th day:	In case of non-submission of report by 28th calendar day, Trading Member shall be disabled in all segments till submission of report.	

Further, trading members are also required to submit closure status of all the non-Compliances reported in Cyber Audit by submitting Corrective Action Taken Report (ATR) i.e., within 3 months from the due date of submission of Preliminary Audit Report. In order to ensure strict adherence for closure of non-Compliances within the prescribed timelines, following penalty as provided in

Table - B shall be Applicable for each High/Medium/Low risk non-compliance, which has not been closed in ATR as per prescribed timelines.

Table – B

Risk rating reported by auditor	**Applicable penalties for each High/Medium/Low risk non-closure of non-Compliances, which have not been closed in ATR (i.e., within prescribed timelines of submission of due date of preliminary audit report)**	
	Non QSB Trading Members	**QSB Trading Members**
High Risk	₹ 50,000	₹ 100,000
Medium Risk	₹ 25,000	₹ 50,000
Low Risk	₹ 5,000	₹ 10,000
In case observations are not closed by Trading Members within three weeks from the due date for submissionof Action Taken Report (ATR), new client registration to be prohibited and notice of 7 days for disablement of trading facility till closure of observation(s). The disablement notice issued to the Trading Member shall be shared with all the Exchanges for information.In case of non-closure of observation(s) within four weeks from the due date of submission of ATR,Trading Member shall be disabled in all segments until closure of observations(s).		