Circular No.: MCX/TECH/605/2024 September 13, 2024

Submission of VAPT report and/or Action taken report (ATR)/Compliance Report

This is with reference to SEBI Circular No-SEBI/HO/MIRSD/TPD/CIR/2022/80 dated June 07, 2022, and Exchange Circulars MCX/TECH/011/2023 dated January 05, 2023, MCX/TECH/641/2023 dated September 25, 2023, MCX/TECH/786/2023 dated November 17, 2023 & MCX/TECH/857/2023 dated December 11, 2023, regarding Submission of VAPT report and/or VAPT compliance report through member portal by all members.

Trading Members are requested to conduct and complete the VAPT during the period September to November for FY 2024-25, in accordance with paragraph/clause 11 (identification of critical assets/applications) & 41 (VAPT) of above-mentioned SEBI circular and the final report after approval from Technology Committee of respective members within one month from the date of completion of VAPT, shall be submitted through enhanced portal to the Stock Exchange.

In view of the above, all trading members shall carry out Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include all critical applications (trading, back office & related activities) and infrastructure components like Servers, Networking systems, Security devices, load balancers pertaining to the activities done as Stock Brokers. The broad area/scope (not limited to) for conduct of VAPT shall also include the following activities:

1. Grey Box assessment of web applications, mobile applications, APIs and thick client applications.
2. Authenticated (wherever possible) Vulnerability Assessment of infrastructure (operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud).
3. External Penetration Testing of all public facing URLs/IPs.
4. Review of network architecture of critical infrastructure.
5. Firewall rule review.
6. Configuration audit of infrastructure (operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud).
7. Wireless penetration testing.

Further, the detailed scope of audit, findings and outcomes of these activities shall be provided in the comprehensive VAPT report along with checklist of test cases providing “FAIL” and “PASS” status.

The detailed VAPT report along with summary of report (as per format specified in Annexure A) as a single document shall be digitally signed by CERT-In empaneled entity to be submitted to Exchange by December 31, 2024, through online Member Portal – https://member.mcxindia.com. Help file ‘VAPT–help file’ is available on the VAPT submission online portal and on https://sftp.mcxindia.com/Common/Online portal help file folder.

---------- Corporate office ----------
Multi Commodity Exchange of India Limited
Exchange Square, CTS 255, Suren Road, Chakala, Andheri (East), Mumbai – 400 093
Tel.: 022 – 6649 4000 Fax: 022 – 6649 4151
www.mcxindia.com email: customersupport@mcxindia.com

Further, as per para 44 of SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, amended vide SEBI Circular No. SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022, 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 within 3 months post the submission of final VAPT report. For any open vulnerabilities as reported & submitted in VAPT report, members are required to submit ATR/Compliance Report (as per format specified in Annexure B) along with Closure report of all the vulnerabilities closed digitally signed by the CERT-In empaneled entity as appointed by the member by March 31, 2025, on member portal. The submission shall be considered complete only if detailed Closure report along with ATR/Compliance report in single file is uploaded on enhanced portal.

In order to ensure strict adherence to the regulatory requirements by members with the prescribed framework applicable for VAPT report and Compliance report for timely closure of vulnerabilities, penalties/disciplinary actions have been prescribed vide circular no MCX/TECH/857/2023 dated December 11, 2023. The details of penalties/disciplinary actions are provided in Annexure C.

For and on behalf of
Multi Commodity Exchange of India Ltd.

Abhay Angarkar
VP-Technology

Annexure – A

VAPT Report Summary				
Name of Trading Member				
Contact person Details (Name, Mobile number & EmailID) of Trading Member (Preferably CISO's)				
VAPT Completion Date "(DD-MM-YYYY)"				
Date of approval of VAPT report by Technology Committee of Trading Member "(DD-MM-YYYY)"				
Name of the Auditor				
Name of the Audit Firm				
Audit Firm Landline No.				
Auditor Mobile No.				
Auditor / Audit Firm Email ID				
CERT-In empanelment validity expiry Date (DD-MM-YYYY)				
Risk	**Critical**	**High**	**Medium**	**Low**
(A) No of closed vulnerabilities				
(B) No of open vulnerabilities				
Reason for non-closure: Mention for Critical, High, Medium, and Low separately				
Vulnerabilities planned to be closed by (DD/MM/YYYY) *				
Remarks				
*Note - As per SEBI Circular dated June 07, 2022, any gaps/vulnerabilities detected shall be remedied on an immediate basis. Further, compliance of closure of findings identified during VAPT shall be submitted within 3 months post submission of VAPT report. The planned target date should be mentioned accordingly.				

Annexure - B

(On the letter head of the CERT-In empaneled entity)

Action Taken Report / Compliance Report on the non-conformities / vulnerabilities identified during the VAPT conducted during the FY._____

Particulars	**Critical**	**High**	**Medium**	**Low**
No. of Open Vulnerabilities as reported in VAPT report submitted to the Exchange				
Current Status				

Explanation / Reason for non-closure

(To be filled in case of open vulnerabilities mentioned in current status)

Details of such open non-Conformities /- Vulnerabilities*	**Explanation / Reason for Non-Closure**

*** Open vulnerabilities shall attract appropriate disciplinary action by the Exchange depending on the criticality / such other factors**

Trading Member (TM) Name & TM Code:	
Auditor Name:	
Name of CERT-In empaneled entity:	
Sign:	

(To be digitally signed by CERT-In empaneled entity as appointed by the Member)

Annexure C

Table A – Non-submission of VAPT report and/or compliance report within below specified dates by Members (other than QSB's):

Details of Violation	**Penalty/Disciplinary actions**	**Penalty/disciplinary action in case of repeated violation**
Non-submission of VAPT report **on or before December 31** and/or Compliance report**on or before March 31**.	1. Charges Rs. 1,500/- per day till first 7 calendar days or submission of report, whichever is earlier. 2. Charges of Rs. 2,500/- per day from the 8th calendar day to 21st calendar day or submission of report, whichever is earlier. 3. 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. 4. The disablement notice issued to the member will be shared with all the Exchanges for information. 5. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%. 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 member will be shared with all the Exchanges for information. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.

Table B – Non-submission of VAPT report and/or compliance report within below specified dates by QSB's Members:

Details of Violation	Penalty/disciplinary actions	Penalty/disciplinary action in case of repeated violation
Non-submission of VAPT report **on or before June 30/December 31** and/or Compliance report **on or before September 30/ March 31.**	1.Charges Rs. 3,000/- per day till first 7 calendar days or submission of report, whichever is earlier 2. Charges of Rs. 5,000/- per day from 8th calendar day to 21st calendar day or submission of report, whichever is earlier 3. In case of non-submission of reporttill 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. 4. The disablement notice issued to the member will be shared with all the Exchanges for information. 5. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%. 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 member will be shared with all the Exchanges for information. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report

Table C – Penalty/Disciplinary actions applicable in case of non-closure of per open vulnerabilities as reported in VAPT report within period of 3 months as specified hereunder: -

Categories of Risks	**For All Members (other than QSBs)**	**For QSB Members**
	Non closure of open vulnerabilities by March31	**Non closure of open vulnerabilities by March 31 (for HY September 30) and by September 30 (for HY March 31)**
High/critica lRisk	Rs.50,000/-	Rs.1,00,000/-
Medium Risk	Rs.25,000/-	Rs.50,000/-
Low Risk	Rs.10,000/-	Rs.20,000/-
Apart from the monetary penalty mentioned above, if **High/Critical/Medium** vulnerability is not closed by member within 21 days from the due date of submission of compliance report, new client registration shall be prohibited and notice of 7 days for disablement of trading facility shall be issued. If the vulnerability is not closed during this notice period, then member shall be disabled in all segments till closure of the vulnerability. The disablement notice issuedto the member will be shared with all the Exchanges for information.		