भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/046 **March 29, 2023**

To

All Portfolio Managers

Association of Portfolio Managers in India (APMI)

Dear Sir / Madam,

Subject: Cyber Security and Cyber Resilience framework for Portfolio Managers

1. With rapid technological advancement in the securities market, there is a greater need for maintaining robust cyber security and to have a cyber-resilience framework to protect the integrity of data and guard against breaches of privacy.

2. As part of the operational risk management, the Portfolio Managers need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in the securities market as Portfolio Manager.

3. Accordingly, all Portfolio Managers with asset under management of INR 3000 crore or more, under discretionary and non-discretionary portfolio management service taken together, as on the last date of the previous calendar month shall comply with the provisions of Cyber Security and Cyber Resilience as placed at **Annexure-1**.

Implementation Schedule:

4. Based on feedback received from stakeholders, it has been decided that the guidelines annexed with this circular shall be effective from October 01, 2023. In this context, Association of Portfolio Managers in India (APMI) shall also furnish activity wise implementation timelines and progress in implementation of provisions of this circular to SEBI on bi-monthly basis.

5. Portfolio Managers and APMI shall take necessary steps for implementing the circular, including putting the required processes and systems in place to ensure compliance with the provisions of this circular.

6. This circular is issued in exercise of powers conferred under Section 11(1) of the Securities and Exchange Board of India Act, 1992 read with Regulation 43 of the SEBI (Portfolio Managers) Regulations, 2020, to protect the interests of

investors in securities market and to promote the development of, and to regulate the securities market.

7. The circular is available on SEBI website at www.sebi.gov.in under the categories “Info for – Portfolio Managers” and "Legal framework - Circulars".

Yours faithfully,

Peter Mardi

Deputy General Manager

+91-22-26449233

peterm@sebi.gov.in

Annexure - 1

1. Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity, and Availability (CIA) of the computer systems, networks, and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). The cyber security framework includes measures, tools, and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operations during, and recover from, a cyber-attack.

Governance

2. As part of the operational risk management framework to manage risk to systems, networks, and databases from cyber-attacks and threats, Portfolio Managers should formulate comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board or equivalent body of the Portfolio Manager, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the Board or equivalent body of the Portfolio Manager at least once annually with the view to strengthen and improve its cyber security and cyber resilience framework.

3. The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risks associated with processes, information, networks, and systems;

   a. 'Identify' critical IT assets and risks associated with such assets,
   b. 'Protect' assets by deploying suitable controls, tools, and measures,
   c. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes,
   d. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack,
   e. 'Recover' from incident through incident management, disaster recovery, and business continuity framework.

4. The Cyber security policy should encompass the principles prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organization (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

5. Portfolio Managers should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

6. Portfolio Managers should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce 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 and resilience policy approved by the Board or equivalent body of Portfolio Manager.

7. The Board or equivalent body of the Portfolio Manager shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a half yearly basis review the implementation of the cyber security and cyber resilience policy approved by their Board or equivalent body, and such review should include a review of their current IT and cyber security and cyber resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board or equivalent body of the Portfolio Manager for appropriate action.

8. The Portfolio Managers should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.

9. The aforementioned committee and the senior management of the Portfolio Manager, including the CISO, should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.

10. Portfolio Managers should define the responsibilities of its employees, outsourced staff, and employees of vendors and other entities, who may have access to or use systems/networks of the Portfolio Managers, towards ensuring the goal of cyber security.

Identify

11. Portfolio Manager shall identify and classify 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 assets. The Board or equivalent body of the Portfolio Manager shall approve the list of critical assets.

To this end, Portfolio Manager shall maintain an up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

12. Portfolio Managers should accordingly 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.

13. Portfolio Managers should also encourage its third-party service providers, if any, such as Custodians, Brokers, Distributors, etc. to have similar standards of Information Security.

Protection

Access Controls

14. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

15. Any access to Portfolio Manager's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Portfolio Manager should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

16. Portfolio Manager should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.

17. Portfolio Managers should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.

18. Portfolio Managers should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallowing privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

19. Account access lock policies after failure attempts should be implemented for all accounts.

20. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Portfolio Manager's critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.

21. Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility.

22. Portfolio Managers 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.

23. Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

24. Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff or visitors should be properly supervised by ensuring at the minimum that outsourced staff or visitors are accompanied at all times by authorized employees.

25. Physical access to the critical systems should be revoked immediately if the same is no longer required.

26. Portfolio Managers should ensure that the perimeter of the critical equipment rooms is 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.

Network Security Management

27. Portfolio Managers should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, and enterprise mobile devices within the IT environment. The Portfolio Manager should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly. The checks should be done at least once in a year.

28. Portfolio Managers should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT

infrastructure from security exposures originating from internal and external sources.

29. Anti-virus software should be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

Security of Data

30. Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA-2, etc.

31. Portfolio Managers 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.

32. The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

33. Portfolio Managers should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

34. Only a hardened and vetted hardware / software should be deployed by the Portfolio Managers. During the hardening process, Portfolio Managers should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments/software.

35. All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

Application Security and Testing

36. Portfolio Managers should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

Patch Management

37. Portfolio Managers should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

38. Portfolio Managers should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of systems and storage devices

39. Portfolio Managers should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

40. Portfolio Managers shall carry out periodic VAPT, inter-alia, including critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as Portfolio Manager, etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

Portfolio Managers shall conduct VAPT at least once in a financial year. However, for the Portfolio Managers, whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year.

Further, all Portfolio Managers shall engage only Indian Computer Emergency Response Team (CERT-In) empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective Portfolio Manager, within 1 month of completion of VAPT activity.

41. Any gaps or vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.

42. In addition, Portfolio Managers 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.

Monitoring and Detection

43. Portfolio Managers should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized 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 should also be monitored for anomalies.

44. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, Portfolio Managers should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.

45. Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

46. Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order 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.

47. The response and recovery plan of the Portfolio Manager should aim at the timely restoration of systems affected by incidents of cyber-attacks or breaches. Portfolio Managers should have Recovery Time Objective (RTO) and Recovery Point Objective (RPO) not more than 4 hours and 30 minutes, respectively

48. The response plan should define responsibilities and actions to be performed by its employees and support or outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.

49. Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

50. Portfolio Managers should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

51. All cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Managers shall be reported to SEBI within 6 hours of noticing/ detecting such incidents or being brought to their notice about such incidents. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the Portfolio Manager, whose systems have been identified as "protected system" by NCIIPC, shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Manager and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/ threats that may be useful for other Portfolio Managers shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year.

    The above information/ reports shall be shared through the dedicated e-mail ids: vapt_reports@sebi.gov.in and cybersecurity_pms@sebi.gov.in

52. Such details as are felt useful for sharing with other Portfolio Managers in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

53. Portfolio Managers should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.

54. The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

55. Portfolio Managers shall arrange to have its systems audited on an annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board or equivalent body of Portfolio Manager within three months of the end of the financial year.

Vendors or Service Providers

56. Portfolio Managers have outsourced many of their critical activities to different agencies / vendors / service providers. The responsibility, accountability and

ownership of those outsourced activities lies primarily with Portfolio Manager. Therefore, Portfolio Manager have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this circular is complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and to certify the above requirement is complied.

****