भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/DOP/CIR/P/2019/111 **October 15, 2019**

To

KYC Registration Agencies

Dear Sir / Madam,

Subject: Cyber Security & Cyber Resilience framework for KYC Registration Agencies

1. Rapid technological developments in securities market have highlighted the need for maintaining robust Cyber Security and Cyber Resilience framework to protect the integrity of data and guard against breaches of privacy.

2. A robust Cyber Security and Cyber Resilience framework should identify the plausible sources of operational risk, both internal and external, and mitigate the impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of its obligation in the event of cyber-attack.

3. Since KYC Registration Agencies (KRAs) perform important function of maintaining KYC records of the clients in the securities market, it is desirable that KRAs have robust Cyber Security and Cyber Resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

4. In view of the above, SEBI's High Powered Steering Committee - Cyber Security decided that the framework on Cyber Security and Cyber Resilience be made applicable for KRAs. The framework placed at **Annexure A**, would be required to be complied by the KRAs with regard to Cyber Security and Cyber Resilience. KRAs are directed to take necessary steps to put in place systems for implementation of this circular by January 01, 2020.

5. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully

D Rajesh Kumar
General Manager
Market Intermediaries Regulation and Supervision Department

Annexure – A

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). Cyber security framework includes measures, tools and processes that are intended to prevent cyber attacks and improve cyber resilience. Cyber Resilience is an organisation's ability to prepare and respond to a cyber attack and to continue operation 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, KRAs should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board of KRAs, 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 of KRAs atleast 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 risk associated with processes, information, networks and systems
   3.1. 'Identify' critical IT assets and risks associated with such assets,
   3.2. 'Protect' assets by deploying suitable controls, tools and measures,
   3.3. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes,
   3.4. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack,
   3.5. 'Recover' from incident through incident management, disaster recovery and business continuity framework.

4. The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (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. KRAs 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. KRAs 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 of the KRAs.

7. The Board of the KRAs shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a quarterly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board, and such review should include 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 of the KRAs for appropriate action.

8. KRAs 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 KRAs, 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. KRAs should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use KRA's systems / networks, towards ensuring the goal of cyber security.

Identify

11. KRAs should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, KRAs should maintain 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. KRAs should accordingly identify cyber risks (threats and vulnerabilities) that it may face, alongwith the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

13. KRAs should also encourage its third-party providers, if any, to have similar standards of Information Security.

Protection

<u>Access Controls</u>

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 KRA's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. KRAs 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. KRAs 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. KRAs 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. KRAs 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, disallow 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 authorised access to the KRA'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. KRAs 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/visitors should be properly supervised by ensuring at the

minimum that outsourced staff/visitors are accompanied at all times by authorised employees.

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

26. KRAs should ensure that the perimeter of the critical equipment room 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.

Network Security Management

27. KRAs 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 KRAs should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

28. KRAs 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. KRAs should implement measures to prevent unauthorised 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. KRAs 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 KRAs. During the hardening process, KRAs 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. KRAs 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. KRAs should establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

38. KRAs 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. KRAs 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. KRAs should regularly conduct vulnerability assessment to detect security vulnerabilities in the IT environment. KRAs should also carry out periodic penetration tests, atleast once in a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

41. Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

42. In addition, KRAs should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces.

Monitoring and Detection

43. KRAs should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised 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, KRAs 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 KRAs should aim at timely restoration of systems affected by incidents of cyber attacks or breaches. KRAs 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.

48. 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.

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

Sharing of information

51. Quarterly reports containing information on cyber attacks and threats experienced by KRAs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other KRAs should be submitted to SEBI in soft copy to kra@sebi.gov.in. The format for submitting quarterly reports is attached as **Annexure B**.

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

Training

53. KRAs 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. KRAs shall arrange to have its systems audited on an annual basis by an CERT-IN empanelled auditor, an independent DISA (ICAI) Qualification, CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (commonly known as (ISC)2), to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of KRAs within three months of the end of the financial year.

****

Annexure - B

Incident Reporting Form	
1. Letter / Report Subject -	
Name of the intermediary - SEBI Registration no. - Type of intermediary -	
2. Reporting Periodicity Year-	
□ Quarter 1 (Apr-Jun) □ Quarter 2 (Jul-Sep)	□ Quarter 3 (Oct-Dec) □ Quarter 4 (Jan-Mar)

3. Designated Officer (Reporting Officer details) -		
Name:	Organization:	Title:
Phone / Fax No:	Mobile:	Email:
Address:		

Cyber-attack / breach observed in Quarter: (If yes, please fill **Annexure C**) (If no, please submit the NIL report)	
Date & Time	Brief information on the Cyber-attack / breached observed

Annexure C	
1. Physical location of affected computer / network and name of ISP -	
2. Date and time incident occurred -	
Date:	Time:

3. Information of affected system -

IP Address:	Computer / Host Name:	Operating System (incl. Ver. / release No.):	Last Patched/ Updated:	Hardware Vendor/ Model:

4. Type of incident -

- □ Phishing
- □ Network scanning /Probing Break-in/Root Compromise
- □ Virus/Malicious Code
- □ Website Defacement
- □ System Misuse

- □ Spam
- □ Bot/Botnet
- □ Email Spoofing
- □ Denial of Service(DoS)
- □ Distributed Denial of Service(DDoS)
- □ User Account Compromise

- □ Website Intrusion
- □ Social Engineering
- □ Technical Vulnerability
- □ IP Spoofing
- □ Ransomware
- □ Other_____

5. Description of incident -

6. Unusual behavior/symptoms (Tick the symptoms) -

- □ System crashes
- □ New user accounts/ Accounting discrepancies
- □ Failed or successful social engineering attempts
- □ Unexplained, poor system performance
- □ Unaccounted for changes in the DNS tables, router rules, or firewall rules
- □ Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic;
- □ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
- □ A system alarm or similar indication from an intrusion detection tool
- □ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server

- □ Anomalies
- □ Suspicious probes
- □ Suspicious browsing New files
- □ Changes in file lengths or dates
- □ Attempts to write to system
- □ Data modification or deletion
- □ Denial of service
- □ Door knob rattling
- □ Unusual time of usage
- □ Unusual usage patterns
- □ Unusual log file entries
- □ Presence of new setuid or setgid files Changes in system directories and files
- □ Presence of cracking utilities
- □ Activity during non-working hours or holidays
- □ Other (Please specify)

7. Details of unusual behavior/symptoms -

8. Has this problem been experienced earlier? If yes, details -

9. Agencies notified -			
Law Enforcement	Private Agency	Affected Product Vendor	Other____________

10. IP Address of apparent or suspected source -	
Source IP address:	Other information available:

11. How many host(s) are affected -		
1 to 10	10 to 100	More than 100

12. Details of actions taken for mitigation and any preventive measure applied -

*****