भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/TPD/P/CIR/2022/95 **July 05, 2022**

To

All KYC Registration Agencies

Dear Sir/ Madam,

Sub: - Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies (KRAs)

1. SEBI vide circular dated 15 October 2019 and 30 May 2022 prescribed framework for Cyber Security and Cyber Resilience for KYC Registration Agencies.

2. In partial modification to Annexure A of SEBI circular dated 15 October 2019 the paragraph-51 shall be read as under:

51. All Cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs shall be reported to SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents.

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 KRAs, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches 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 shall be submitted to SEBI within 15 days from the quarter ended June, September, December

*and March of every year. The above information shall be shared through the dedicated e-mail id: **kra@sebi.gov.in**. The format for submitting the quarterly reports is attached as **Annexure B**.*

3. KRAs shall take necessary steps to put in place systems for implementation of the circular.

4. The provisions of the Circular shall come into force with immediate effect.

5. The circular is issued with the approval of the competent authority.

6. 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,

Vishal M Padole
Deputy General Manager
MIRSD
Tel. No: 022 26449247
Email ID: vishalp@sebi.gov.in

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 3 (Oct-Dec)	
☐ Quarter 2 (Jul-Sep)	☐ 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 -

*****