भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/DOP/CIR/P/2019/110 **October 15, 2019**

To

Registrars to an Issue / Share Transfer Agents

Dear Sir / Madam,

Subject: Cyber Security & Cyber Resilience framework for Qualified Registrars to an Issue / Share Transfer Agents

1. SEBI, vide circular SEBI/HO/MIRSD/CIR/P/2017/100 dated September 08, 2017, prescribed the framework for Cyber Security & Cyber Resilience for Qualified Registrars to an Issue / Share Transfer Agents (QRTAs).

2. Paragraph 51 of Annexure A of the SEBI circular dated September 08, 2017 specifies the following regarding sharing of information:

   Quarterly reports containing information on cyber-attacks and threats experienced by QRTAs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other QRTAs should be submitted to SEBI in soft copy to rta@sebi.gov.in.

3. In this regard, following guidelines are being issued for submission of report / information and the timelines:
   3.1. A format for submitting the reports is attached as Annexure.
   3.2. For the quarter ended on September 30, 2019, quarterly reports shall be submitted by QRTAs not later than November 30, 2019 as per the format specified.
   3.3. Effective from quarter ending on December 31, 2019, the time period for submission of the report shall be 15 days after the end of the quarter.
   3.4. The mode of submission of reports by QRTAs to SEBI shall be through email.

4. 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

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure

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 I**) (If no, please submit the NIL report)		
Date & Time	Brief information on the Cyber-attack / breached observed	

Annexure I	
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 -

*****