CDSL/OPS/DP/POLCY/2019/535 **October 23, 2019**

CYBER SECURITY & CYBER RESILIENCE FRAMEWORK FOR STOCK BROKERS / DEPOSITORY PARTICIPANTS - CLARIFICATIONS

This is with reference to the CDSL circular CDSL/OPS/DP/POLCY/2019/375 dated July 06, 2019 and SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 on Cyber Security & Cyber Resilience framework for Stock Brokers / Depository participants.

SEBI has issued circular No. SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019 on the captioned subject wherein they have provided the clarification on the periodicity of the cyber security audit and the qualification of the Auditor. The format for submitting the quarterly report on the cyber attacks and threats has also been specified. The copy of the said SEBI circular is enclosed as **Annexure-A**.

In view of the above, all Members shall submit the report in the revised format, duly signed by the Designated Officer appointed in terms of para 6 of the Annexure-1 of the said SEBI Circular dated December 03, 2018. The format of the quarterly report as specified by SEBI is enclosed in **Annexure-B**. The report for the quarter ending on September 30, 2019 shall be submitted on or before November 30, 2019. Members who have already submitted the details of any Cyber attack/threat/incident for the quarter ending on September 2019 are advised to resubmit the same in the revised format by the due date. Henceforth, effective from quarter ending on December 2019, time period for submission of the report shall be 15 days after the end of the respective quarter.

CDSL will modify the provision to submit the report in electronic interface which shall be notified by a separate circular within November 15, 2019. Members are requested to submit the information through electronic interface only.

All Members are advised to take note and comply.

In case of any queries, members can send mail to dpinfosec@cdslindia.com or helpdesk@cdslindia.com

sd/-

Rajesh Nadkarni
Chief Information Security Officer

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/DOP/CIR/P/2019/109 **October 15, 2019**

To

All Recognised Stock Exchanges
Depositories – NSDL and CDSL

Dear Sir / Madam,

Subject: Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants - Clarifications

1. SEBI, vide circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, prescribed the framework for Cyber Security & Cyber Resilience for Stock Brokers / Depository Participants.

2. Paragraph 52 of Annexure 1 of the SEBI circular dated December 03, 2018 specifies the following regarding sharing of information:

   Quarterly reports containing information on cyber-attacks and threats experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants should be submitted to Stock Exchanges / Depositories.

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 stock brokers / depository participants 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 such reports by the stock brokers / depository participants may be prescribed by Stock Exchanges / Depositories.

4. With regard to periodic audit as specified in paragraph 58 of Annexure 1 of the SEBI circular dated December 03, 2018, it has been decided that auditors qualified in following certifications can audit the systems of depository participants and stock brokers to check the compliance of Cyber Security and Cyber Resilience provisions:

   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]).

5. The periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience provisions for depository participants shall be annual. The periodicity of audit for the compliance with the provisions of Cyber Security and Cyber Resilience provisions for stock brokers, irrespective of number of terminals and location presence, shall be as under:

Type of stock broker as specified in SEBI circular CIR/MRD/DMS/34/2013 dated November 06, 2013	Periodicity
Type I	Annual
Type II	Annual
Type III	Half-yearly

Paragraph 58 of Annexure 1 of the SEBI circular dated December 03, 2018 stands modified accordingly.

6. Stock Exchanges and Depositories shall
   a) make necessary amendments to the relevant byelaws, rules and regulations for the implementation of the above direction;
   b) bring the provisions of this circular to the notice of their members and depository participants respectively and also disseminate the same on their websites; and
   c) communicate to SEBI, the status of implementation of the provisions of this circular in their Monthly Report.

7. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 and Section 19 of the Depositories Act 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 Member / Depository Participant - Name of the Stock Exchange / Depository - Member ID / DP ID -			
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 -

*****

Annexure

Incident Reporting Form			
1. Letter / Report Subject -			
Name of the Member / Depository Participant - Name of the Stock Exchange / Depository - Member ID / DP ID -			
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 -