Annexure - A

Form for sharing information on Cyber Security incident

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

Annexure 1
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 -