



Incident Reporting Form		
1. Letter / Report Subject -		
Name of the intermediary - SEBI Registration no. - Type of intermediary -		
2. Reporting Periodicity Year-		
<input type="checkbox"/> Quarter 1 (Apr-Jun)	<input type="checkbox"/> Quarter 3 (Oct-Dec)	
<input type="checkbox"/> Quarter 2 (Jul-Sep)	<input type="checkbox"/> 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 -				
<input type="checkbox"/> Phishing <input type="checkbox"/> Network scanning /Probing Break-in/Root Compromise <input type="checkbox"/> Virus/Malicious Code <input type="checkbox"/> Website Defacement <input type="checkbox"/> System Misuse	<input type="checkbox"/> Spam <input type="checkbox"/> Bot/Botnet <input type="checkbox"/> Email Spoofing <input type="checkbox"/> Denial of Service(DoS) <input type="checkbox"/> Distributed Denial of Service(DDoS) <input type="checkbox"/> User Account Compromise	<input type="checkbox"/> Website Intrusion <input type="checkbox"/> Social Engineering <input type="checkbox"/> Technical Vulnerability <input type="checkbox"/> IP Spoofing <input type="checkbox"/> Ransomware <input type="checkbox"/> Other_____		
5. Description of incident -				
6. Unusual behavior/symptoms (Tick the symptoms) -				
<input type="checkbox"/> System crashes <input type="checkbox"/> New user accounts/ Accounting discrepancies <input type="checkbox"/> Failed or successful social engineering attempts <input type="checkbox"/> Unexplained, poor system performance <input type="checkbox"/> Unaccounted for changes in the DNS tables, router rules, or firewall rules <input type="checkbox"/> Unexplained elevation or use of privileges <input type="checkbox"/> Operation of a program or sniffer device to capture network traffic; <input type="checkbox"/> An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user <input type="checkbox"/> A system alarm or similar indication from an intrusion detection tool <input type="checkbox"/> Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	<input type="checkbox"/> Anomalies <input type="checkbox"/> Suspicious probes <input type="checkbox"/> Suspicious browsing New files <input type="checkbox"/> Changes in file lengths or dates <input type="checkbox"/> Attempts to write to system <input type="checkbox"/> Data modification or deletion <input type="checkbox"/> Denial of service <input type="checkbox"/> Door knob rattling <input type="checkbox"/> Unusual time of usage <input type="checkbox"/> Unusual usage patterns <input type="checkbox"/> Unusual log file entries <input type="checkbox"/> Presence of new setuid or setgid files <input type="checkbox"/> Changes in system directories and files <input type="checkbox"/> Presence of cracking utilities <input type="checkbox"/> Activity during non-working hours or holidays <input type="checkbox"/> 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 -

--
