NCIIPC Incident Report Form

Type of Report	Initial/Follow-up/Final	Classification of Document	Restricted/Confidenti

Section-A: General Information

1. Organisation Details	
Name of CI	
Address of CI	
Name of CISO	
Contact Details of CISO	
Contact Details of Office handling the incident	

2. Date Incident Occurred		Approximate Time	

3. Type of Incident(✓Check mark)

	Website Defacement		Un-patched Vulnerable Software Exploitation
	Patched Software Exploitation		Unauthorised System Access
	Exploitation of Weak Configuration		Data Theft
	Account Compromise		Malware Infection
	Service Disruption		Wireless Access point Exploitation
	Social Engineering and Phishing Attacks		Exploitation of Weak Network Architecture
	Unintentional Information Exposure		Network Penetration
	Spoofing or DNS Poisoning		Any other (Please describe below)

4. Brief description of the incident

5. Interface affected		Public Network		Internal Network		Other

6. Incident Handling Steps taken	
a) Immediate	
b) Long term	
c) Was System backup plan implemented successfully? If yes, details of the Backup Plan applied	

7. Whether other agencies such as CERT have also been informed? If yes, please mention here

(Use Separate Sheet for additional information)

Section-B: CII Information

8. CII assets affected					
9. Impact of Incident on CIIs(✓Check mark)					
	Data theft		Service Disruption (Downtime)		
	System (software/hardware) Sabotage		Other (please explain)		
10. Number of Users affected					
11. Duration of Incident	from	(dd/mm/yyyy, hh:mm)	to	(dd/mm/yyyy, hh:mm)	
12. Impact on dependent ICT					
13. Threat Profile					
a) Attacking IP address					
b) Source port of attacking machine					
14. Type of attack(✓Check mark)					
	Denial of Service		Unauthorised Access (internal or external)		
	Malware attack		Website Defacement		
	Phishing attack		Other		
15. Root Cause Analysis (with following details)					
a) Log analysis Report					
b) Forensic Report					
c) Audit Report					
d) Network traffic Analysis Report					
Details of Compromised Machine					
a) Physical Location					
b) Operating System					
c) IP Address					
d) MAC Address					
e) DNS Entry					
f) Domain/Workgroup					
g) Is the compromised machine connected to a network?		Yes		No	
h) Is the compromised machine connected to a modem?		Yes		No	
i) Physical Security details of the machine		Yes		No	
j) Logical Security details of the machine		Yes		No	
k) Was the compromised machine had to be removed from the		Yes		No	
16. Current Status of the Incident					
(Use Separate Sheet for additional information)					
17. Was Crisis Management Plan Offered? Please explain the details					
(Use Separate Sheet for additional information)					