



NCIIPC Incident Report Form

Type of Report		Classification of Document	
----------------	--	----------------------------	--

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 attack(✓ Check mark)

<input type="checkbox"/> Website Defacement	<input type="checkbox"/> Un-patched Vulnerable Software Exploitation
<input type="checkbox"/> Patched Software Exploitation	<input type="checkbox"/> Unauthorised System Access
<input type="checkbox"/> Exploitation of Weak Configuration	<input type="checkbox"/> Data Theft
<input type="checkbox"/> Account Compromise	<input type="checkbox"/> Malware Infection
<input type="checkbox"/> Service Disruption	<input type="checkbox"/> Wireless Access point Exploitation
<input type="checkbox"/> Social Engineering and Phishing Attacks	<input type="checkbox"/> Exploitation of Weak Network Architecture
<input type="checkbox"/> Unintended Information Exposure	<input type="checkbox"/> Network Penetration
<input type="checkbox"/> Spoofing or DNS Poisoning	<input type="checkbox"/> 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)			
<input type="checkbox"/> Data theft	<input type="checkbox"/> Service Disruption (Downtime)		
<input type="checkbox"/> System (software/hardware) Sabotage	<input type="checkbox"/> 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)			
<input type="checkbox"/> Denial of Service	<input type="checkbox"/> Unauthorised Access (internal or external)		
<input type="checkbox"/> Malware attack	<input type="checkbox"/> Website Defacement		
<input type="checkbox"/> Phishing attack	<input type="checkbox"/> Other (Explain)		
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?	<input type="checkbox"/>	Yes	No
h) Is the compromised machine connected to a modem?	<input type="checkbox"/>	Yes	No
i) Physical Security details of the machine	<input type="checkbox"/>	Yes	No
j) Logical Security details of the machine	<input type="checkbox"/>	Yes	No
k) Was the compromised machine had to be removed from the network?	<input type="checkbox"/>	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)			