NCIIPC Responsible Vulnerability Disclosure

1. Reporter's Details			
a) Full Name			
b) Email			
c) Organisation/Company			
2. Vulnerability Details (✓Check mark)			
a) Vulnerability Name			
b) Vulnerability category	☐ XSS	☐ SQLI	☐ Stack Overflow
	☐ LFI	☐ Click Jacking	☐ User After Free
	☐ XSRF	☐ Information Leakage	☐ Heap Overflow
	☐ Insecure Direct Object Reference	☐ Broken Authentication	
	☐ Memory Corruption	☐ Security Misconfiguration	
c) Description (Use Separate Sheet for additional information)			

3. Type of Vulnerability (✓Check mark)	☐ Web Application	☐ Operating System(OS)
	☐ SCADA	☐ Any Other
If other please describe in brief		
4. Date when issue found	(dd/mm/yyyy)	
5. Steps to reproduce		

6. Whether POC screenshots/files/documents attached?	☐ Yes	☐ No
7. Reported to Affected Organisation?	☐ Yes	☐ No
8. Affected Organisation's name		
9. Affected Organisation's URL		
10. Affected Organisation's email		

11. Vulnerable Product type	☐ Web Application	☐ Client Software
	☐ Server Software	☐ Firmware
	☐ Operating System	☐ Hardware
12. Vulnerable Product name & Version		
13. If reported, Email ID to whom details sent		
14. If reported, date when reported		
15. Patch released?	☐ Yes	☐ No
16. If patch released, date of patch release	(dd/mm/yyyy)	
17. Anonymity	(Yes/No)	