Cybersecurity Incident Report Form

Cybersecurity Incident Informer Details

Report #		**Report Date**	
Incident Informer Name		**Position**	
Department/Sector		**Email Address**	
Mobile #/Landline #		**Incident #**	
Incident Discovery Date		**Incident Reporting Date**	

Cybersecurity Incident Details

Cybersecurity Incident Type (Choose * for all that apply)

	Account Compromise (e.g., Lost Password)		Misuse of Systems (e.g., Acceptable Use)
	Denial-of-Service (Including Distributed)		Reconnaissance (e.g., Scanning, Probing)
	Malicious Code (e.g., Virus, Worm, Trojan)		Social Engineering (e.g., Phishing, Scams)
	Theft/Loss of Equipment or Media		Technical Vulnerability (e.g., 0-day Attacks)
	Unauthorized Access (e.g., Systems, Devices)		Ransomware (e.g., Shamoon, Petya)
	Other (Please specify):		

Cybersecurity Incident Description

Cybersecurity Incident Root Cause Analysis

CS Incident Priority (* CS Incident Priority = CS Incident Urgency*CS Incident Impact)

Low □	Medium □	High □

Impact Type (Choose * for all that apply)

	Loss of Access to Services		Propagation to Other Networks
	Loss of Productivity		Unauthorized Disclosure of Information
	Loss of Reputation		Unauthorized Modification of Information
	Loss of Revenue		Personal Safety/Security
	Unknown		Other (Please specify):

Systems Affected by CS Incident

Attack Sources (e.g., IP Address, Port):	
Attack Destinations (e.g., IP address, Port):	
IP Addresses of Affected Systems:	

Primary Functions of Affected Systems: (e.g., Web Server, Domain Controller)			
Operating Systems of Affected Systems: (e.g., Version, Service Pack, Configuration)			
Security Software Loaded on Affected Systems: (e.g., Anti-Virus, Anti-Spyware, Firewall, Versions, Date of Latest Definitions)			
Physical Location of Affected Systems: (e.g., State, City, Building, Room, Desk)			
CS Incident Suggested Remediation Actions			
Short Term Actions	1.		
Long Term Actions	1.		
Incident Remediation Responsibility			
Name	**Department/Sector**	**Expected Closure Date**	**Signature**
Does CS Incident Resolved?	Yes, Totally Resolved □	Partially Resolved □	No, Not Resolved □
Incident Remediation needs Assistant or Escalation to an external party or NCA			
Yes **(* please specify the external party name)** □		No □	