

Preparation to Handle Network Security Incidents

Note: Prior to starting the preparation of handle network security incidents checklist, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, if Applicable, Extension:			
<i>Additional Details (If Any):</i>			

Section 3: Checklist of Preparation Steps for Handling Network Security Incidents	
Actions	Completed
Whether the network perimeter control devices such as firewalls, IDS, and IPS are configured to log all the access attempts, and send notification of any intrusion attempt to administrator	<input type="checkbox"/>
Whether syslog or any other centralized logging mechanism is implemented to backup logs from all network security devices at a single place	<input type="checkbox"/>
Whether the roles and responsibilities of all users, administrators, and IH&R team members are clearly defined for the incident response process to maintain secure access to the network infrastructure.	<input type="checkbox"/>
Whether standard network usage protocols are implemented	<input type="checkbox"/>
Whether necessary training is provided and conducted practice sessions for the team members to verify their efficiency	<input type="checkbox"/>
Whether necessary tools are prepared for assisting detection and containment of the threat	<input type="checkbox"/>
Whether network sniffing tools, security solutions, and other logging tools across all network servers are installed to record all incoming and outgoing traffic and alert administrators about current incidents	<input type="checkbox"/>
Whether backups from all the important servers are taken properly and kept them accessible	<input type="checkbox"/>
Whether employee monitoring applications (if allowed under legal and policy frameworks) are used to check for inappropriate resource usage.	<input type="checkbox"/>
Whether internet service providers (ISPs) and their second-tier agents are contacted to gather information about the incident handling and response processes for the network incidents on their end	<input type="checkbox"/>
Whether the goals of the IH&R process are communicated and whether a backup network ready for emergencies	<input type="checkbox"/>
Whether the contact details of national and government security organizations, such as CERT and the Internet Crime Complaint Center (IC3) are kept ready to seek help in case of attacks that can affect national security	<input type="checkbox"/>
Have the human resources and legal departments collaborated to frame fair usage policies for all employees.	<input type="checkbox"/>

Whether the physical security team has been informed regarding the behavior of internal users and trained to report all discrepancies	<input type="checkbox"/>
Whether network infrastructure administrators are contacted to discuss methods they can use to assist in analyzing and containing network-based DoS and DDoS attacks	<input type="checkbox"/>
Whether a process is designed for interviewing a perpetrator with the help of legal authorities, as the perpetrators may be mentally unstable or become violent on confrontation	<input type="checkbox"/>
Whether a legal department from the IH&R team is formed that would handle liability issues and incidents targeting customers, clients, and third-party service providers	<input type="checkbox"/>
Whether the legal department members can obtain proper permission before informing the victims about the incident and clearly understand the knowledge they need to reveal	<input type="checkbox"/>
Whether the organizations are logging user activities, such as FTP commands, web requests, and email headers with the help of proxies, application logs, and network-based IDPS sensors	<input type="checkbox"/>
Whether the IH&R team configured IDS and IPS software to detect DoS traffic	<input type="checkbox"/>
Whether the intrusion detection method with the ISPs is discussed to restrict the attacker's access to organizational resources	<input type="checkbox"/>
Whether live analysis laboratory configurations are defined and host hardening and sandbox environments are determined	<input type="checkbox"/>
Whether the capture requirements are estimated and the type of capture required (e.g., limited capture, full packet capture) is identified while performing network data capturing	<input type="checkbox"/>
Whether appropriate capture device deployment locations are determined and ensured the network's integrity and security after introducing a capture device	<input type="checkbox"/>
Whether a secure storage facility is maintained to store the evidence and other critical information	<input type="checkbox"/>
Whether the cryptographic hashes of critical files are kept in-hand to increase the speed of analysis, verification, and eradication	<input type="checkbox"/>
Whether spare workstations, hosts, clean OS, networking equipment, and virtualized tools are developed, which can be used for restoring backups, recovery, etc.	<input type="checkbox"/>