

Eradication of Network Security Incidents Checklist

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 Received:	Report		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 for Eradicating Unauthorized Access Incidents	
Actions	Completed
Check whether the physical security measures are implemented to restrict access to critical resources	<input type="checkbox"/>
Check hardware, programs, networks, and data at an organizational level are secured	<input type="checkbox"/>
Ensure proper physical security measures are deployed in the required areas to safeguard the information assets	<input type="checkbox"/>
Ensure that no networking devices and cables are physically accessible without proper surveillance	<input type="checkbox"/>
Check whether the appropriate password policy is prepared	<input type="checkbox"/>
Check whether strong authentication is implemented for accessing critical resources	<input type="checkbox"/>
Check whether all default passwords are changed to highly secured and complex passwords	<input type="checkbox"/>
Check whether the authentication and authorization standards for employees are created	<input type="checkbox"/>
Check whether procedures for provisioning and de-provisioning user accounts are deployed	<input type="checkbox"/>
Check whether the CAPTCHA system to mitigate brute-force attacks is deployed	<input type="checkbox"/>
Check whether all the components of the incident from systems was eliminated	<input type="checkbox"/>
Ensure to perform various security assessments to identify vulnerabilities and risks	<input type="checkbox"/>
Check whether the unwanted services on hosts are disabled	<input type="checkbox"/>
Check account lockout mechanism is applied to prevent the system from brute-force attacks on passwords	<input type="checkbox"/>
Ensure to run services with the least privileges possible to reduce the immediate impact of successful exploits	<input type="checkbox"/>
Ensure to use host-based/personal firewall software to limit the exposure of the individual host to attacks	<input type="checkbox"/>
Limit unauthorized physical access to logged-in systems by requiring hosts to lock idle screens automatically and asking users to log off before leaving the office	<input type="checkbox"/>

Check whether regularly verifying the permission settings for critical resources, including password files, sensitive databases, and public web pages	<input type="checkbox"/>
Check whether the systems are restored or reinstall that suffered a root compromise	<input type="checkbox"/>
Check whether the network is design to block suspicious traffic	<input type="checkbox"/>
Check whether a virtual-private-network (VPN) gateway is employed to separate the remote VPN traffic from the local network	<input type="checkbox"/>
Ensure to secure all remote access methods, including modems and VPNs	<input type="checkbox"/>
Check whether all publicly accessible systems and services are moved to a secured demilitarized zone (DMZ)	<input type="checkbox"/>
Check whether all unwanted services are disabled	<input type="checkbox"/>
Check whether centralized logging for all users is configured	<input type="checkbox"/>

Section 4: Checklist for Eradicating Inappropriate Usage Incidents

Actions	Completed
Check whether the firewall and IDS/IPS are installed to block services that violate organizational policy	<input type="checkbox"/>
Check whether the email servers are configured to block outbound spam	<input type="checkbox"/>
Ensure to install spam filter software to block spam messages to and from internal users	
Check whether the URLs are filtered to prevent access to inappropriate or malicious websites by creating a web proxy server that runs URL filtering software	<input type="checkbox"/>
Check whether the network firewall is configured to send outgoing requests through proxy servers	<input type="checkbox"/>
Check whether the outbound connections are limited and are using encrypted protocols, such as Secure Shell (SSH), HTTP Secure (HTTPS), and IP Security Protocol (IPsec)	<input type="checkbox"/>
Register the user activity logs and keep monitoring them regularly	<input type="checkbox"/>
Always store sensitive data in remote servers and restrict its access	<input type="checkbox"/>
Check whether authentication is enabled for sharing files across the network	<input type="checkbox"/>

Check whether the latest data protection and Internet usage policies are enforced	<input type="checkbox"/>
Ensure that systems with the latest security updates are patched	<input type="checkbox"/>
Check whether any unauthorized software is uninstalled	<input type="checkbox"/>
Check whether USB debugging is disabled and disallow the use of untrusted sources	<input type="checkbox"/>
Check whether strong authentication Implemented for accessing critical resources	<input type="checkbox"/>

Section 5: Checklist for Eradicating DoS/DDoS Incidents

Actions	Completed
Check whether ingress filtering, egress filtering, TCP intercept, and rate limiting methods are deployed to block various potential DoS/DDoS attacks	<input type="checkbox"/>
Check whether botnets are disabled using techniques such as RFC 3704 filtering, black-hole filtering, DDoS prevention offerings from ISP or DDoS service	<input type="checkbox"/>

Section 6: Checklist for Eradicating Wireless Network Security Incidents

Actions	Completed
Check whether a complex passphrase of a minimum of 20 characters in length is selected and change it at regular intervals	<input type="checkbox"/>
Check whether Wi-Fi Protected Access 3 (WPA3) security protocol is used for wireless networks	<input type="checkbox"/>
Check whether VPN technology is used such as remote access, extranet, and intranet VPN systems	<input type="checkbox"/>
Check whether network access control (NAC) or network access protection (NAP) solution are Implement for additional control over end-user connectivity	<input type="checkbox"/>
Check whether auto updates for all wireless devices and patch the device firmware are turned on	<input type="checkbox"/>
Check whether the device is connected to an unprotected network while accessing sensitive resources	<input type="checkbox"/>

Check whether the HTTPS Everywhere extension and two-factor authentication is enabled	<input type="checkbox"/>
Ensure to block the switch port to which the access point (AP) is connected or manually locate the AP and physically remove it from the LAN	<input type="checkbox"/>
Ensure to use non-regular patterns as PIN keys while pairing a device	<input type="checkbox"/>
Check whether any unknown and unexpected request for a pairing of a device is restricted	<input type="checkbox"/>
Check whether multi-factor authentication (MFA), extensible authentication protocol (EAP), and IEEE standard (IEEE 802.1X) are employed across the network	<input type="checkbox"/>
Check whether a static IP address is used for the wireless network	<input type="checkbox"/>
Check whether universal plug and play (UPnP) protocol is disabled from the devices connected to the wireless network	<input type="checkbox"/>
Check whether AP software is updated and installed with the latest patches	<input type="checkbox"/>
Check whether MAC filtering is applied to allow only known devices into the network	<input type="checkbox"/>
Check whether the VLAN isolation is implemented to separate the network and place the devices on a specific VLAN	<input type="checkbox"/>