

Recovery of Network Security Incidents Checklist

Note: Prior to starting the recovery of 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: Recovery after Unauthorized Access Incidents Checklist	
Actions	Completed
Whether the data is recovered from backup files in case of data loss	<input type="checkbox"/>
Whether all the systems are restored to the ready-to-work state	<input type="checkbox"/>
Whether all systems are patched and updated with the latest software version	<input type="checkbox"/>
Whether the affected files are replaced with clean files from backups	<input type="checkbox"/>
Whether the files are deleted that were added or created by the attacker	<input type="checkbox"/>
Whether it is confirmed that the affected systems are functioning normally	<input type="checkbox"/>
Whether additional monitoring is implemented to look for related activity in the future	<input type="checkbox"/>
Whether the security policies and protection mechanisms are formulated and regularly updated	<input type="checkbox"/>
Whether the perimeter security, such as updating the rules of firewalls, IDS/IPS are tightened	<input type="checkbox"/>
Whether the DNS cache entries are cleared	<input type="checkbox"/>
Section 4: Recovery after Inappropriate Usage Incidents Checklist	
Actions	Completed
Whether the situation is communicated to the organization's legal department representatives regarding liability issues	<input type="checkbox"/>
Whether the human resource and legal department representatives are consulted regarding the procedures for handling inappropriate usage incidents	<input type="checkbox"/>
Whether proper training to the employees is provided to ensure proper usage and understand the legal liabilities of such incidents	<input type="checkbox"/>
Whether the employees are trained to verify site security before trying to login or upload personal or professional details onto it	<input type="checkbox"/>
Whether proper guidelines and policies regarding downloading objectionable content using the organization's system and networks are provided	<input type="checkbox"/>
Whether the antivirus database is updated	<input type="checkbox"/>
Whether additional third-party security solutions are implemented to identify users acting inappropriately	<input type="checkbox"/>

Whether protective monitoring of critical services is implemented to identify inappropriate activity	<input type="checkbox"/>
Whether loading of unusual drivers is blocked	<input type="checkbox"/>
Whether the latest data encryption policy is implemented to protect data from unauthorized users	<input type="checkbox"/>
Whether regular security audits are conducted to reduce network security risks	<input type="checkbox"/>
Whether the systems and applications are updated to the latest software version	<input type="checkbox"/>
Section 5: Recovery after DoS/DDoS Incidents Checklist	
Actions	Completed
Whether the extent of the impact on different resources, their ability to function, and the risks involved in using the compromised resources are determined	<input type="checkbox"/>
Whether various methods of recovery are devised depending on the severity of the incident, systems affected, critical systems and devices required to keep the business running, and backup resources available	<input type="checkbox"/>
Whether proper communication is made with the incident response team to select the best recovery plan and obtain the required permissions from cybersecurity authorities	<input type="checkbox"/>
Whether the backup resources are used efficiently to replace the compromised systems	<input type="checkbox"/>
Whether the lost data is recovered from backup files	<input type="checkbox"/>
Whether all systems are restored to their ready-to-work state	<input type="checkbox"/>
Whether the functionality of all restored systems is properly checked	<input type="checkbox"/>
Whether additional monitoring is implemented to look for related activity in future	<input type="checkbox"/>
Whether the security policies are formulated and regularly updated	<input type="checkbox"/>
Whether the unwanted DDoS detection logs recorded across the security solutions are erased after detecting and responding to a DDoS attack	<input type="checkbox"/>
Whether the Border Gateway Protocol (BGP) protocol is restarted to send a keepalive message after restoring the website from the DoS attack	<input type="checkbox"/>
Whether an automated communication desk is established to keep in touch with the clients once the DDoS attack is resolved	<input type="checkbox"/>

Whether a strategy is developed to establish connections to the clients involving different data centers after restoring the server	<input type="checkbox"/>
Whether the best DDoS mitigation strategy is implemented, and the ISP provider is demonstrated to unblock the blocked services during the attack	<input type="checkbox"/>
Whether an orderly restoration of applications is planned after rectifying the DDoS attack to avoid secondary attack situations while restarting applications	<input type="checkbox"/>
Section 6: Recovery after Wireless Network Security Incidents Checklist	
Actions	Completed
Whether a random passphrase is selected that is not made up of dictionary words	<input type="checkbox"/>
Whether the client settings are properly configured	<input type="checkbox"/>
Whether all routers and Wi-Fi devices are updated with the latest security patches	<input type="checkbox"/>
Whether SSID broadcasts are disabled	<input type="checkbox"/>
Whether the default SSID is changed after the WLAN configuration	<input type="checkbox"/>
Whether SSID cloaking is used to keep certain default wireless messages from broadcasting the ID to everyone	<input type="checkbox"/>
Whether SSID including company name, network name, or any easy-to-guess string in passphrases is avoided	<input type="checkbox"/>
Whether the router access password is set, and firewall protection is enabled	<input type="checkbox"/>
Whether firewall or packet filter is placed in between the AP and the corporate intranet	<input type="checkbox"/>
Whether the remote router login and wireless administration are disabled	<input type="checkbox"/>
Whether MAC address filtering on the AP or router is enabled	<input type="checkbox"/>
Whether encryption on the access points is enabled, and the passphrase is changed often	<input type="checkbox"/>
Whether the strength of the wireless network is limited so it cannot be detected outside the bounds of the organization	<input type="checkbox"/>
Whether the wireless devices is regularly checked for configuration or setup problems	<input type="checkbox"/>
Whether an additional technique is implemented for encrypting traffic, such as IPsec over wireless networks	<input type="checkbox"/>

Whether Wi-Fi protected access 3 (WPA3) is selected instead of WPA and WPA2	<input type="checkbox"/>
Whether WPA3 Enterprise is implemented wherever possible	<input type="checkbox"/>
Whether the network is disabled when not required	<input type="checkbox"/>
Whether a centralized server is used for authentication	<input type="checkbox"/>
Whether Bluetooth is kept in the disabled state, and enabled it only when needed for the duration of the intended task	<input type="checkbox"/>
Whether the Bluetooth device is kept in non-discoverable (hidden) mode	<input type="checkbox"/>
Whether all Bluetooth devices that are paired with the network in the past are checked and unknown devices are deleted	<input type="checkbox"/>
Whether encryption is enabled when establishing a Bluetooth connection to your PC	<input type="checkbox"/>
Whether the Bluetooth-enabled device is set to the lowest network range and perform pairing only in a secure area	<input type="checkbox"/>
Whether antivirus is installed that supports host-based security software on Bluetooth-enabled devices	<input type="checkbox"/>
Whether the default settings of the Bluetooth-enabled device are changed to the best security standard	<input type="checkbox"/>
Whether link encryption is used for all Bluetooth connections	<input type="checkbox"/>
Whether the wireless router is reset to default configurations after the attack and the password are changed to take control of the router's admin console and network	<input type="checkbox"/>
Whether the WPS (Wi-Fi protected setup) functionality is disabled	<input type="checkbox"/>
Whether the router DNS settings is reset and changed	<input type="checkbox"/>
Whether it is ensured that the affected wireless network and systems are functioning normally	<input type="checkbox"/>
Whether the router's guest network option is enabled	<input type="checkbox"/>