

Eradication of Mobile-based Security Incidents Checklist

Note: Prior to starting the eradication of mobile-based security incidents, 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:			

Section 3: Checklist for Eradicating Mobile-based Security Incidents	
Actions	Completed
Ensure to perform repeated scans to completely remove the malware from the organization's network and devices.	<input type="checkbox"/>
Check whether remote wiping techniques are used to delete organizational data from the devices.	<input type="checkbox"/>
Check whether the identified vulnerabilities are patched in the devices to prevent similar incidents.	<input type="checkbox"/>
Check whether automated antivirus scans are running to remove the malware.	<input type="checkbox"/>
Check whether strange or suspicious applications are uninstalled.	<input type="checkbox"/>
Check whether lost device tracking service is enabled.	<input type="checkbox"/>
Check whether mobile antivirus and security apps are installed such as Norton Mobile Security, McAfee Mobile Security, and Kaspersky Antivirus & VPN.	<input type="checkbox"/>
Check whether built-in security features are enabled on both Android and iOS devices.	<input type="checkbox"/>
Check whether sensitive data from the mobile devices are removed before reissuing them to other users.	<input type="checkbox"/>
Check whether the affected devices are analyzed and build the eradication plan with zero or minimum integral damage to the organization.	<input type="checkbox"/>
Check whether saved webpages, passwords, and downloaded files are deleted to avoid reinfecting the device.	<input type="checkbox"/>
Check whether suspected add-on services, notifications, and browser extensions are disabled on the device.	<input type="checkbox"/>
Check whether the device is turned off and switched to safe/emergency mode to eradicate the malware without triggering it.	<input type="checkbox"/>
Check whether temporary files are deleted and cleared the recycle bin.	<input type="checkbox"/>
Check whether the impact of the malware on other devices is eliminated with the help of the remote access feature.	<input type="checkbox"/>
Check whether access to applications or services used by the employees is controlled and limited.	<input type="checkbox"/>

Check whether the operating system or applications are reinstalled in case the malware is persistent in nature.	<input type="checkbox"/>
Check whether after removing malware, the applications are updated and the functionalities of the device are restored.	<input type="checkbox"/>