

Containment of Mobile-based Security Incidents Checklist

Note: Prior to starting the containment 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 Containing Mobile-based Security Incidents	
Actions	Completed
Check whether the mobile devices are isolated by disconnecting them from the organization's network and shutting them down.	<input type="checkbox"/>
Check whether the passwords of the bank, email, social media, and other online accounts that use multi-factor authentication are changed.	<input type="checkbox"/>
Check whether the passwords of all cloud-based services are changed.	<input type="checkbox"/>
Check whether the old SIM card is deactivated and blocked by contacting the provider.	<input type="checkbox"/>
Check whether malware detection tools are running to identify the affected applications.	<input type="checkbox"/>
Check whether the compromised applications are removed or uninstalled.	<input type="checkbox"/>
Check whether complete information is gathered, including the apps installed, operating system version, and type of device.	<input type="checkbox"/>
Check whether browser cache, cookies, and history are deleted.	<input type="checkbox"/>
Check whether all accounts related to the employee are blocked until the incident is resolved.	<input type="checkbox"/>
Check whether unauthorized permissions granted to the application are blocked and ensure to revoke the associated services.	<input type="checkbox"/>
Check whether the remote wipe features are utilized to remove malware from the infected mobile devices.	<input type="checkbox"/>
Check whether the mobile device is rebooted into safe mode to isolate malicious applications.	<input type="checkbox"/>
Check whether unwanted communication is blocked with the outside network.	<input type="checkbox"/>
Check whether vulnerable services are stopped and ensure to block access to the company resources.	<input type="checkbox"/>
Check whether compromised mobile devices are disposed safely without exposure to any data theft.	<input type="checkbox"/>
Check whether security check-ups are performed to fix any security issues in the mobile device and user account.	<input type="checkbox"/>