

Preparation for Handling Mobile-based Security Incidents Checklist

Note: Prior to starting the preparation for handling mobile-based 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: | | | |

| Section 3: Preparation Steps to Handle Mobile-based Security Incidents | |
|--|--------------------------|
| Actions | Completed |
| Whether a strict mobile device security policy is implemented | <input type="checkbox"/> |
| Whether the mobile asset management is incorporated, including operating systems, their versions, and applications installed | <input type="checkbox"/> |
| Whether mobile devices' usage is constantly monitored for any compliance violations | <input type="checkbox"/> |
| Whether the information collected from mobile devices is correlated with known intelligence to determine the risks | <input type="checkbox"/> |
| Whether a workstation is prepared with the necessary tools for effective mobile incident response | <input type="checkbox"/> |
| Whether regular backup data is created and stored in a secure location to avoid data loss in case of mobile device failure or loss | <input type="checkbox"/> |
| Whether mobile application management (MAM) solution is deployed to manage employees' devices | <input type="checkbox"/> |
| Whether the security controls are configured properly to get alerts about mobile device use and associated applications | <input type="checkbox"/> |
| Whether the data acquisition strategies are properly defined for performing mobile forensics | <input type="checkbox"/> |
| Whether the necessary tools are accumulated for mobile malware analysis | <input type="checkbox"/> |
| Whether remote wiping capabilities are implemented to prevent data leakage | <input type="checkbox"/> |
| Whether the communication means are established to report lost or stolen devices | <input type="checkbox"/> |
| Whether a list of contractors or vendor mobile devices that have access to business systems is created | <input type="checkbox"/> |

Preparation for Handling Mobile-based Security Incidents Checklist

| | |
|---|--------------------------|
| Whether the isolation and communication plans are created for mobile incident response | <input type="checkbox"/> |
| Whether the roles and responsibilities of the IH&R team members are properly defined for mobile-based incident handling | <input type="checkbox"/> |
| Whether the automation for mobile-based security and the IH&R process are implemented | <input type="checkbox"/> |
| Whether the network architecture is reviewed for proper mobile incident management | <input type="checkbox"/> |
| Whether the MDM and IAM tools are deployed to detect various mobile security incidents at the earliest | <input type="checkbox"/> |
| Whether the security policies are implemented to prevent jailbroken or rooted mobile devices from accessing company resources | <input type="checkbox"/> |