Incident Response Playbook

Stolen Devices

Phase 1: Preparation

Set the parameters for the response team's and the incident response plan's (IRP) scope.

Determine the criticality of each asset and the associated risk.

Create a communication strategy to alert important stakeholders in case an issue arises.

Create a strategy for incident reporting and escalation, including how to report a stolen device.

Define the Incident Response Team's duties and functions.

Create a training schedule for the Incident Response Team and any necessary people.

Set up standards for data backup and recovery.

Put security measures in place to stop unauthorized access to devices and data.

Phase 2: Detection and Analysis

Inform the Incident Response Team right away if a gadget is reported stolen.

Gather details about the stolen gadget, including its make, model, serial number, and location information.

Identify the size of the data breach and evaluate the risk to the company.

Find out whether any additional equipment or systems have been impacted.

To ascertain how the device was stolen, examine logs and other pertinent data.

Inform the proper law enforcement agencies and provide them any pertinent details about the stolen equipment.

Consult an attorney to provide legal guidance on the occurrence.

Phase 3: Containment, Eradication, and Recovery

All user names and passwords associated with the impacted device should be changed.

Start the process of retrieving the stolen data from backups.

Restore the impacted gadget to its prior state.

Implement new security measures to stop thefts in the future.

Work with law police to retrieve the stolen device and any potentially compromised data.

Engage the law office to offer legal guidance during the recovery process.

Phase 4: Post Incident Activity

Review the occurrence to ascertain what worked and what didn't.

Create a lesson plan and update the incident response plan as needed.

Give important stakeholders a report on the situation.

Inform and educate every employee about the theft and how to avoid it in the future.

For any indications of illegal access or usage, keep an eye on the impacted device and its data.

Assist the law firm in making certain that all requisite legal and regulatory standards have been satisfied.

Update law enforcement often on the recovery's status and any new information that may come to light.