ChecklistGuro

Cybersecurity Incident Case Management Checklist Template

Show only Checklist

Display Style
Default

Detection & Reporting

Initial steps after a potential incident is identified.

Date of Detection

Enter date...

Time of Detection

Enter time...

Detection Method

- [ ] SIEM Alert
- [ ] User Report
- [ ] Endpoint Detection
- [ ] Network Intrusion Detection
- [ ] Other

Initial Description of Incident

Write something...

Severity Score (if applicable)

Enter a number...

Reported By

- [ ] User
- [ ] Automated System
- [ ] 3rd Party

Containment

Actions to limit the scope and impact of the incident.

Affected System(s) Tier

- [ ] Tier 1 (Critical)
- [ ] Tier 2 (Important)
- [ ] Tier 3 (Minor)

Systems Isolated

- [ ] Web Servers
- [ ] Database Servers
- [ ] Email Servers
- [ ] Workstations
- [ ] Network Devices

Number of Systems Isolated

Enter a number...

Isolation Start Date

Enter date...

Isolation Start Time

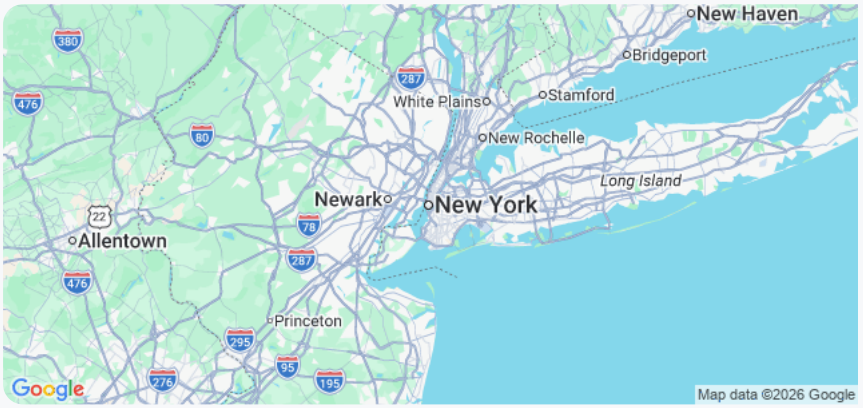
Enter time...

Containment Actions Description

Write something...

Isolation Zone Location

Set My Current Location



Eradication

Removing the root cause of the incident.

Root Cause Analysis Summary

Write something...

Vulnerability Exploited (if applicable)

- [ ] Malware
- [ ] Phishing
- [ ] SQL Injection
- [ ] Zero-Day Exploit
- [ ] Misconfiguration
- [ ] Unknown

Number of Affected Systems

Enter a number...

Malware Sample (if applicable)

Upload File

Remediation Steps Taken

Write something...

Patch Status (for Affected Systems)

- [ ] Patched
- [ ] Not Patched
- [ ] Pending Patch

Recovery

Restoring affected systems and data.

System Restoration Start Date

Enter date...

System Restoration Start Time

Enter time...

Percentage of Systems Recovered

Enter a number...

Detailed Description of Recovery Actions Taken

Write something...

Data Integrity Verification Method

- [ ] Automated Scripts
- [ ] Manual Verification
- [ ] Third-Party Tool

Data Verification Completion Date

Enter date...

Description of any Data Loss or Corruption

Write something...

Post-Incident Activity

Reviewing the incident, documenting lessons learned, and improving security posture.

Summary of Incident Root Cause

Write something...

Detailed Timeline of Events

Write something...

Affected Systems/Assets

- [ ] Server A
- [ ] Database B
- [ ] Endpoint C
- [ ] Network Segment D

Estimated Financial Impact ($)

Enter a number...

Date of Post-Incident Review

Enter date...

Recommendations for Improvement

Write something...

Incident Severity Level (Reassessed)

- [ ] Low
- [ ] Medium
- [ ] High
- [ ] Critical

Legal & Compliance

Tasks related to legal requirements, reporting obligations, and data privacy.

Applicable Data Breach Laws?

- [ ] GDPR
- [ ] CCPA
- [ ] HIPAA
- [ ] State Data Breach Laws
- [ ] Other (Specify in Long Text)

Specific Legal/Regulatory Requirements?

Write something...

Date of Legal Consultation?

Enter date...

Estimated Number of Affected Individuals

Enter a number...

Notification Requirements?

- [ ] Attorney General
- [ ] Affected Individuals
- [ ] Credit Reporting Agencies
- [ ] Media

Summary of Legal Review and Advice

Write something...

Legal Consultation Documentation

Upload File

Communication

Internal and external communications related to the incident.

Communication Method

- [ ] Email
- [ ] Phone
- [ ] SMS
- [ ] Instant Messaging

Initial Communication Draft

Write something...

Stakeholders to Notify

- [ ] Legal Team
- [ ] PR Department
- [ ] Executive Management
- [ ] Affected Users

Date of First Communication

Enter date...

Time of First Communication

Enter time...

Contact Person Details (Recipient)

Write something...

Evidence Preservation

Steps to preserve forensic evidence for investigation.

Date and Time of Evidence Collection

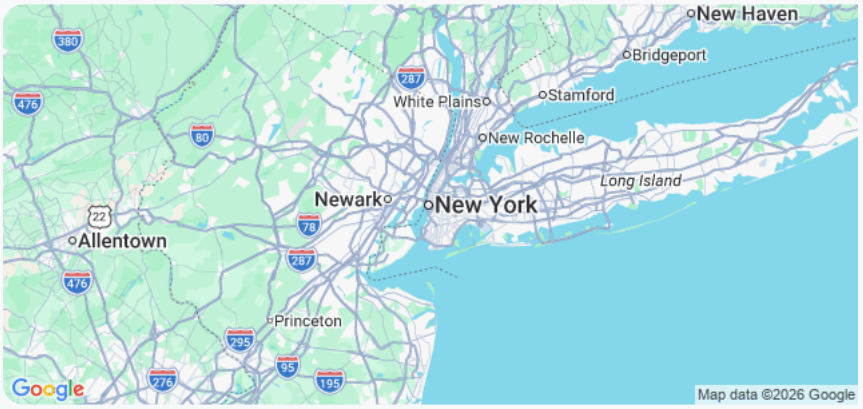
Enter date...

Exact Time of Evidence Collection

Enter time...

Location of Evidence Found

Set My Current Location



Detailed Description of Evidence

Write something...

Photos/Screenshots of Evidence

Upload File

Signature of Evidence Collector

Chain of Custody Record Number

Write something...