# Security Incident Report Template

|  |  |  |
| --- | --- | --- |
| Start Date/Time | End Date/Time | Duration |
| Text | Text | Text |

### Purpose

Use this section to explain briefly why this report is being filled out (i.e. what incident is it addressing?). Try to describe the incident in just one sentence.

E.g. *The purpose of this report is to provide details around the recent [X-type] incident that occurred at [Organization].*

### Audience

Use this section to indicate for whom this report is intended.

### Summary of Incident

Give a brief recap of the incident in three to five sentences. This section provides a succinct description of the following:

* Why this occurred (no more than one sentence).
* How many users were impacted, and what departments, regions, and stores were impacted.
* What was the outcome (short term, e.g. ERP outage for five hours).
* What type of incident it was.

### Threat Escalation Protocol Information

Use this section to document the incident’s scope and impact and to indicate if the appropriate response procedure was followed.

E.g. This incident was classified as a Tier 2 incident, given that it was a medium impact level and medium scope.

Please refer to the [*Information Security Incident Management Plan*](https://www.infotech.com/research/information-security-incident-management-plan) for further information on the definitions of impact and scope.

Note: To change the highlighted impact/scope cell, right click the currently highlighted cell and select “borders” from the formatting menu that appears. Then, click on “Borders and Shading” at the bottom of the list. From here, you can adjust the border type; reset the currently highlighted cell’s borders to match the surrounding ones, and then repeat the process for the cell you wish to highlight, but select a thicker border so it stands out.

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Escalation Protocol** | | | |
| **Impact** | **Scope** | | |
| **High** | **Medium** | **Low** |
| **High** | **Tier 1** | **Tier 1** | **Tier 2** |
| **Medium** | **Tier 2** | **Tier 2** | **Tier 2** |
| **Low** | **Tier 2** | **Tier 3** | **Tier 3** |

The Security Incident Response Team’s (SIRT) self-evaluation has indicated that the proper response process was followed and the tier was identified in the correct amount of time.

### Timeline of Response Actions

Use this section to document what actions were taken during the remediation and when they occurred. Unlike in the [*Root-Cause Analysis Template*](https://www.infotech.com/research/root-cause-analysis-template)*,* stick to only the high-level details. Provide no more than five critical points/highlights of the incident response actions.

|  |  |
| --- | --- |
| Date | Details |
| Monday August 5, 2019 |  |
| Tuesday August 6, 2019 |  |
| Thursday August 8, 2019 |  |
| Friday August 9, 2019 |  |

### Damages and/or Business Impact

Describe the following; add or remove questions as needed:

* What is the associated monetary cost of the incident?
* To what extent did the incident disrupt normal operations?
* Was any data permanently lost? If so, what is the value of that data?
* Was any hardware damaged? If so, what is the value of that damage?
* Did the incident cause reputational damage to the business?

### Assumptions and Future Changes

Review the questions below and summarize the incident response quality. Highlight assumptions the SIRT made during the remediation process and how these assumptions will be adjusted for future incidents.

* Was the incident preparation sufficient?
* Was detection prompt? Why/why not?
* What should be done differently if this incident were to reoccur?
* Did staff adequately deal with the incident with respect to their assigned roles and responsibilities?

### Closing Statement

Use this section to highlight the response action and area(s) of improvement and recommendations for achieving those needed changes.

### Incident Response Contacts

|  |  |
| --- | --- |
| **Contact** | **Contact Information** |
| **Third Party/Vendor** |  |
| **Security** |  |
| **IT Operations** |  |
| **CISO** |  |
| **HR** |  |
| **Communications** |  |
| **SOC** |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.