[Company name]

How to use this document: delete this paragraph before saving, sharing, or circulating it. Every part shown in blue is yours to replace: type your own details over each blue [field] until no blue remains. Add or remove table rows to fit your needs. Then select all (Ctrl+A) and set the font colour to the same dark colour throughout. What is left is your finished document.

# IT Incident Report Form

*The factual record of one incident: what happened, who was affected, what fixed it, and what happens next.*

## 1. Incident details

| | |
|---|---|
| **Incident reference number** | [Incident reference number] |
| **Title of this incident** | [Title of this incident] |
| **Date and time the incident started** | [Date and time the incident started] |
| **Date and time the incident was detected** | [Date and time the incident was detected] |
| **Date and time service was restored** | [Date and time service was restored] |
| **Person reporting this incident** | [Full name of the person reporting this incident] |
| **Incident lead** | [Full name of the incident lead] |
| **Severity of this incident** | [Severity of this incident, with the meaning of that level] |
| **Status of this incident** | [Status of this incident: open, contained, resolved, or closed] |

## 2. Summary

[Summary of this incident in two or three sentences: what stopped working, for whom, and for how long.]

## 3. Impact

| | |
|---|---|
| **Systems and services affected** | [List of the systems and services affected] |
| **Users or locations affected** | [Description of the users or locations affected] |
| **Number of users affected** | [Number of users affected, or confirmation that the number is not yet known] |
| **Business effect of this incident** | [Description of the business effect of this incident] |
| **Data lost or exposed** | [Confirmation of whether data was lost or exposed, and how that is known] |

## 4. Timeline

Record events in time order, using one time zone throughout, stated here: [Time zone used in this timeline]. Add or remove rows as needed.

| Date and time | Event, action, or decision | Person responsible | Evidence or reference |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**[Company name]**

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 5. Cause

[Confirmed cause of this incident, or confirmation that the cause is not yet known.]

[Contributing factors that made this incident more likely or more severe.]

[Questions still open about the cause, and who is pursuing each one.]

## 6. Response and resolution

[Immediate actions taken to contain this incident and limit its impact.]

[Fix that restored service, and anything that is still temporary rather than permanent.]

[Workaround given to affected users while service was unavailable.]

## 7. Evidence preserved

[Location where logs, screenshots, and other evidence for this incident are stored.]

[Reference numbers for any related tickets, alerts, or monitoring records.]

## 8. Follow-up actions

Each action needs an owner and a due date. Add or remove rows as needed.

| Follow-up action | Owner of this action | Due date for this action | Status of this action |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 9. Lessons and prevention

[Lesson learned from this incident.]

[Change that will prevent a repeat, or reduce its impact, and the action number it relates to in section 8.]

## 10. Sign-off

| | |
|---|---|
| **Incident lead name** | [Full name of the incident lead] |
| **Reviewer name** | [Full name of the reviewer] |

## [Company name]

| | |
|---|---|
| **Incident lead signature** | [Signature of the incident lead] |
| **Reviewer signature** | [Signature of the reviewer] |
| **Date of sign-off** | [Date of sign-off] |