# [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. 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:** _____ **Title of this incident:** _____

**Date and time the incident started:** _____ **Date and time the incident was detected:** _____

**Date and time service was restored:** _____ **Person reporting this incident:** _____

**Incident lead:** _____ **Severity of this incident:** _____

**Status of this incident:** _____

**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:** _____ **Users or locations affected:** _____

**Number of users affected:** _____ **Business effect of this incident:** _____

**Data lost or exposed:** _____

**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 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**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:** _____ **Reviewer name:** _____

**Incident lead signature:** _____ **Reviewer signature:** _____

**Date of sign-off:** _____