IT incident: the first hour

Grade it, run it, record it. Severity matrix, first-hour checklist and the UK personal data check.

1. Grade it: impact × urgency

Impact ↓ / Urgency →	Now	Soon	Can wait
Widespread	P1	P2	P3
Significant	P2	P3	P4
Limited	P3	P4	P4

Widespread	Most staff or clients, a whole site, or a client-facing service is down
Significant	One team, one client or one important system is affected or badly degraded
Limited	One person or a few
Now	Harm is growing, or a deadline or contract target is at risk today, and no workaround stops it
Soon	A workaround holds for a few hours, but it must be fixed today
Can wait	Inconvenient, not getting worse

Overrides

Personal data may be involved
At least P2. Start the breach record now: the 72-hour clock runs from when you become aware.

Security may be compromised
At least P2. Preserve evidence (logs, the affected machine) before anyone wipes or rebuilds.

You are not sure
Grade it higher. Downgrading later costs nothing; under-grading costs the first hour.

2. What each priority means

P1 Critical
Respond: 15 minutes · Updates: every 30 minutes
Log + major incident report (MIR) within 1 working day + post-incident review within 5 working days + summary to directors and affected clients

P2 High
Respond: 30 minutes · Updates: every hour
Log + incident report within 1 working day; review if it ran over 4 hours or is a repeat

P3 Medium
Respond: 4 working hours · Updates: when resolved
Log entry with a closing note

P4 Low
Respond: next working day · Updates: when resolved
Log entry

3. The first hour

1. Log it: an ID, when it started (best estimate), when and how you found out, who reported it.
2. Grade it on the matrix. Three people reporting the same fault is not three small incidents.
3. P1 or P2: name one incident manager to coordinate and talk, so the fixers can fix.
4. Tell people within the response time, and say when the next update will come.
5. Keep the timeline as you go: time, what happened, and where you saw it.
6. Security in doubt? Keep the evidence: no wiping, rebuilding or restoring over it yet.
7. Run the personal data check (section 4) and note the time you became aware.

4. Personal data check (UK GDPR, as at November 2026: check ico.org.uk)

Personal data involved?
Names, emails, HR or customer records, anything about a person. Loss of access can count, not only leaks. If none: normal log.

▶

Unlikely risk to people
Do not report. Record it in your breach log with the reasons. Every breach is recorded.

▶

Risk is likely
Report to the ICO without undue delay and within 72 hours of becoming aware. Send what you know; add the rest later.

▶

High risk to people
Also tell the people affected without undue delay: what happened, the likely effect, what you are doing.

Processing data for a client? Tell that client (the controller) without undue delay; the reporting decision is theirs. A cyber attack is also a crime: report it to the police (England, Wales and Northern Ireland: Report Fraud, 0300 123 2040; Scotland: Police Scotland, 101). ICO breach advice line: 0303 123 1113.

5. Hold a post-incident review when

- Every P1, without exception
- Any P2 that lasted more than four hours, or repeated a cause seen in the last 90 days
- Any suspected personal data breach or security compromise, whatever its priority
- Any P1 to P3 incident that a person reported before your monitoring noticed
- Anyone involved asks for one

© Garrould Limited · CC BY-NC 4.0 · Share freely for non-commercial use with a link to https://www.itmanagement101.co.uk/it-incident-report-template/
Full templates (Word, Excel) and the worked example at the link. General guidance, not legal advice.