CLOUDSWITCHED

FREE RESOURCE — INCIDENT RESPONSE TEMPLATE

IT Incident Response Template

Structured template for documenting, escalating and resolving major IT incidents. Capture every detail from initial declaration to post-incident review so consistent handling, clear communication and a thorough lessons-learned land on every P1 or P2 event.

5	72hr	100%	Fillable
RESPONSE PHASES COVERED	ICO NOTIFICATION DEADLINE	INCIDENTS SHOULD BE DOCUMENTED	TICK & TYPE IN ANY VIEWER

P1 / P2 INCIDENTS · GDPR AWARE · POST-MORTEM · AUDIT-READY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this template

Open this template for every **P1 or P2 incident** and start filling it in the moment the incident is declared — not after the dust settles. Update in real time during the response. Once the incident is closed, conduct a structured post-mortem within five business days and attach the completed template to your incident management system. This is an **interactive PDF** — tick the boxes and type into the fillable lines directly in any modern viewer.

WHAT THIS TEMPLATE IS

A consistent, audit-ready record of how a single major IT incident was identified, classified, contained, resolved and reviewed. It captures the timeline, the decisions, the people involved, and the lessons learned — the evidence pack you need for ICO breach reporting, cyber insurance claims, customer notifications, and internal governance.

DATA BREACH — THE 72-HOUR RULE

Under UK GDPR, if an incident involves a **personal data breach that poses a risk to individuals**, you must notify the ICO within 72 hours of becoming aware. Section 3 below includes the assessment fields. If in doubt, escalate to your DPO or legal counsel and document the rationale either way.

The five response phases

- **01 Incident Identification** — reference, reporter, commander, priority, affected systems and users.
- **02 Classification & Escalation** — incident category, escalation log, stakeholders informed.
- **03 Containment & Mitigation** — real-time action log, plus the UK GDPR 72-hour decision.
- **04 Resolution & Recovery** — root cause, restoration time, verification checklist.
- **05 Post-Incident Review** — what happened, what worked, what to improve, follow-up actions.

Roles to agree first

Assign these four roles before you start. The Commander is the single point of decision; everyone else reports up.

- **Incident Commander** — owns the response and the call on escalation, comms and resolution.
- **Technical Lead** — drives containment and recovery; reports status to the Commander.
- **Communications Lead** — user notifications, stakeholder updates and any regulator contact.
- **Scribe** — keeps this template up to date in real time as events happen.

01

Incident Identification

Record the initial details of the incident as soon as it is reported or detected. The Scribe should start filling this section the moment the Incident Commander declares the response open.

Incident details

Incident reference _____

Date & time reported _____

Reported by _____

Method of report _____

Incident Commander _____

Priority (P1 / P2 / P3) _____

Incident description

Provide a clear, factual summary — what happened, what systems and services are affected, how many users are impacted.

_____

_____

_____

_____

Impact assessment

Systems affected _____

Users impacted (number) _____

Business functions affected _____

Data breach suspected (Y/N) _____

Revenue impact (est.) _____

Regulatory notification required _____

02

Classification & Escalation

Classify the incident type and document the escalation path followed. Decide who needs to know based on category, and capture every escalation in the log below with a real time stamp.

Classification reference

CATEGORY	EXAMPLES	ESCALATION REQUIRED
Service Outage	Email down, internet failure, server crash	Immediate — all stakeholders
Security Incident	Ransomware, phishing compromise, data breach	Immediate — security team + management
Hardware Failure	Server disk failure, switch failure, UPS alarm	Within 30 minutes — IT team + vendor
Software Failure	Application crash, database corruption	Within 1 hour — IT team + vendor
Network Issue	Connectivity loss, high latency, DNS failure	Within 30 minutes — IT team + ISP

Escalation log

Capture each escalation as it happens. The Scribe owns this table.

TIME	ESCALATED TO	METHOD	RESPONSE RECEIVED

ESCALATION RULE OF THUMB

If an incident is going to affect customer-facing services or trigger any regulatory clock, escalate *up* early. Late escalation is the single most common failure pattern in post-incident reviews.

03

Containment & Mitigation

Document every action taken during containment — who did what, when, and what happened. This log is critical for the post-incident review and may be required for regulatory or insurance purposes.

Action log

TIME	ACTION TAKEN	PERFORMED BY	RESULT

DATA BREACH — THE 72-HOUR RULE

Under UK GDPR, if the incident involves a **personal data breach that poses a risk to individuals**, you must notify the ICO within 72 hours of becoming aware. Document your assessment of whether notification is required and the rationale for your decision either way — that record is itself evidence.

Containment decision

Containment achieved (Y/N) _____

Time contained _____

ICO notification required (Y/N) _____

Rationale & decision-maker _____

04

Resolution & Recovery

Document how the incident was resolved and services restored to normal operation. Verify each item on the recovery checklist before declaring closure — an "it's probably fine" is not closure.

Resolution details

Root cause identified _____

Resolution description _____

Service restored (date / time) _____

Confirmed by _____

Users notified (date / time) _____

All systems verified _____

Recovery verification checklist

- ☐ All **affected systems** are back online and functioning normally.
- ☐ **Monitoring** confirms services are stable with no recurring errors.
- ☐ Affected **users have confirmed** they can work normally.
- ☐ **Backup jobs** have resumed and completed successfully.
- ☐ **Security scans** confirm no residual threats or vulnerabilities.
- ☐ Temporary **workarounds removed** and permanent fixes applied.

> **DEFINITION OF RESOLVED**
>
> An incident is closed when the underlying cause is fixed (not just symptoms suppressed), monitoring is clean for the agreed bake-in period, end users have explicitly confirmed normal service, and the temporary workarounds you put in during containment have been removed.

05

Post-Incident Review

Conduct a structured review within five business days of incident closure. Involve all key participants — the Commander, the Technical Lead, the Comms Lead and at least one affected user representative. The goal is honest learning, not blame.

Review meeting

Review date _____

Review attendees _____

1. What happened?

Provide a factual timeline of events from first detection to full resolution. Cross-check against the action log on page 04.

2. What went well?

Identify aspects of the response that worked effectively — people, process, tooling, communication. Note these so they are reinforced, not just remembered.

3. What could be improved?

Identify gaps in the response process, communication, or tooling. Be specific — "monitoring" is not an answer, "no alert on disk >90% on the file server" is.

Actions & sign-off

Capture every follow-up action with a named owner and a real deadline. An action without an owner is a wish — an action without a deadline is procrastination. Then sign off this incident as closed.

4. Required actions

ACTION	OWNER	DEADLINE	STATUS

PREPARED BY	DATE	APPROVED BY

CLOUDSWITCHED

INCIDENT RESPONSE & IT RESILIENCE

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom