CLOUDSWITCHED

FREE RESOURCE — TEMPLATE

# IT Incident Response Template

Structured template for documenting, escalating, and resolving IT incidents. Ensure consistent handling, clear communication, and thorough post-incident review for every major IT event.

| 6 | 72hr | 100% | Free |
|---|---|---|---|
| RESPONSE PHASES COVERED | ICO NOTIFICATION DEADLINE | INCIDENTS SHOULD BE DOCUMENTED | READY TO USE TEMPLATE |

**How to Use This Template**

Complete this template for every P1 or P2 incident. Begin filling in details as soon as the incident is declared. Update in real-time during the response. Conduct a post-incident review within 5 business days and attach this completed document to your incident management system.

## 1 Incident Identification

Record the initial details of the incident as soon as it is reported or detected.

**Incident Reference:** .....

**Date & Time Reported:** .....

**Reported By:** .....

**Method of Report:** .....

**Incident Commander:** .....

**Priority Level (P1/P2/P3):** .....

### Incident Description

Provide a clear, factual summary of the incident. What happened? What systems/services are affected? How many users are impacted?

**Notes**

.....

.....

.....

.....

### Impact Assessment

**Systems Affected:** .....

**Number of Users Impacted:** .....

**Business Functions Affected:** .....

**Data Breach Suspected (Y/N):** .....

**Revenue Impact (Est.):** .....

**Regulatory Notification Required:** .....

## 2 Incident Classification & Escalation

Classify the incident type and document the escalation path followed.

| CLASSIFICATION | 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

| TIME | ESCALATED TO | METHOD | RESPONSE RECEIVED |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## 3 Containment & Mitigation

Document the immediate actions taken to contain the incident and prevent further damage.

Record every action taken during the containment phase, including who performed it and when. This log is critical for post-incident review and may be required for regulatory or insurance purposes.

| TIME | ACTION TAKEN | PERFORMED BY | RESULT |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Data Breach: 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.

## 4 Resolution & Recovery

Document how the incident was resolved and services restored to normal operation.

**Root Cause Identified:** .....

**Resolution Description:** .....

**Notes**

.....

.....

.....

**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 have been removed and permanent fixes applied

## 5 Post-Incident Review

Conduct a structured review within 5 business days of incident closure. Involve all key participants.

**Review Date:** .....

**Review Attendees:** .....

### Review Questions

**1. What happened?** Provide a factual timeline of events from first detection to full resolution.

**Notes**

.....

.....

**2. What went well?** Identify aspects of the response that worked effectively.

**Notes**

.....

.....

**3. What could be improved?** Identify gaps in the response process, communication, or tooling.

**Notes**

.....

.....

**4. What actions are required?** Document specific, measurable actions with owners and deadlines.

| ACTION | OWNER | DEADLINE | STATUS |
|---|---|---|---|





Prepared By: ..... Date: ..... Approved By: .....