CLOUDSWITCHED

FREE RESOURCE — TEMPLATE

Security Incident Response Plan

Detection, containment, eradication, recovery, and post-incident review. Build a structured incident response capability that minimises damage and recovery time from security incidents.

6	72hr	Zero	Free
RESPONSE PHASES	ICO NOTIFICATION DEADLINE	TARGET DWELL TIME	RESPONSE PLAN TEMPLATE

How to Use This Template

Customise this template for your organisation, assign roles, and conduct a tabletop exercise to test it before an incident occurs. Store copies digitally (cloud) and physically (printed, off-site). Review after every incident and at least annually.

1 Plan Overview & Roles

Organisation: .....

Plan Version: .....

Last Review Date: .....

Plan Owner: .....

Incident Response Team

ROLE	PRIMARY	BACKUP	CONTACT NUMBER
Incident Commander			
IT Lead / Technical Lead			
Communications Lead			
Legal / DPO			
Senior Management Sponsor			
External IR Provider			

Incident Severity Levels

SEVERITY	DEFINITION	RESPONSE TIME	EXAMPLES
Critical	Active attack, data breach, ransomware, complete outage	Immediate (within 15 min)	Ransomware encryption active, confirmed data exfiltration
High	Significant security event, potential data exposure	Within 1 hour	Compromised admin account, malware detected on multiple devices
Medium	Security event contained, limited impact	Within 4 hours	Single phishing compromise (contained), suspicious network activity
Low	Minor security event, no immediate threat	Within 24 hours	Failed phishing attempt, low-risk vulnerability discovered

2 Phase 1: Detection & Identification

Detect the incident and assess its nature, scope, and severity.

- [ ] The incident has been **detected** via: user report, monitoring alert, vendor notification, or external report
- [ ] The **incident type** has been identified: malware, phishing, unauthorised access, data breach, DDoS, insider threat
- [ ] The **scope** has been assessed: affected systems, users, data, and business functions
- [ ] The **severity level** has been assigned based on the classification above
- [ ] The **Incident Commander** has been notified and has assumed responsibility
- [ ] The **incident response team** has been assembled (physically or virtually)
- [ ] An **incident log** has been started recording all actions, times, and decisions
- [ ] Initial **evidence has been preserved** (screenshots, log exports, memory dumps)

3 Phase 2: Containment

Stop the incident from spreading while preserving evidence for investigation.

- [ ] **Short-term containment:** Isolate affected systems from the network (disconnect, disable accounts)
- [ ] **Network isolation:** Block malicious IPs, domains, and email addresses at the firewall
- [ ] **Account containment:** Reset passwords for compromised accounts, revoke active sessions
- [ ] **Communication blackout:** Do not alert the attacker — do not use compromised systems to communicate
- [ ] Affected systems have been **forensically imaged** before any remediation (if possible)
- [ ] **Backup integrity** has been verified — confirm backups are not compromised
- [ ] Legal/DPO has been notified to assess **regulatory notification** requirements

4 Phase 3: Eradication & Recovery

Remove the threat completely and restore systems to normal operation.

- [ ] **Root cause** has been identified — how did the attacker get in?
- [ ] **Malware/backdoors** have been removed from all affected systems
- [ ] **Vulnerability** that was exploited has been patched or mitigated
- [ ] **Compromised credentials** have all been reset (not just the initially discovered ones)
- [ ] Systems are **rebuilt or restored** from known-good backups (not just cleaned)
- [ ] **Enhanced monitoring** is in place to detect any re-compromise attempts
- [ ] Systems are brought **back online gradually** with testing at each stage
- [ ] Users are **notified** when systems are restored and any actions they need to take

5 Phase 4: Regulatory Notification

- [ ] **ICO notification assessment:** Does this breach pose a risk to individuals? If yes, notify within 72 hours.
- [ ] **Data subject notification:** If high risk to individuals, notify affected data subjects without undue delay.
- [ ] **Action Fraud:** Report if the incident involves a crime (fraud, hacking, ransomware).
- [ ] **NCSC:** Report significant cyber incidents to the National Cyber Security Centre.
- [ ] **Cyber insurance:** Notify your insurer as per policy requirements (often within 24–48 hours).
- [ ] **Affected third parties:** Notify any customers, suppliers, or partners whose data may have been compromised.

72-Hour ICO Deadline

Under UK GDPR, you must notify the ICO within 72 hours of becoming aware of a personal data breach that poses a risk to individuals. This deadline is strict. Document your decision-making process whether or not you decide to notify. Failure to notify when required can result in fines of up to £8.7 million or 2% of global turnover.

6 Phase 5: Post-Incident Review

Review Date (within 5 business days): .....

Review Attendees: .....

- [ ] A **timeline of events** has been compiled from detection through resolution
- [ ] **Root cause** and contributing factors are documented
- [ ] **What worked well** in the response has been identified
- [ ] **What needs improvement** has been identified with specific actions
- [ ] **Action items** have been assigned with owners and deadlines
- [ ] The **incident response plan** has been updated based on lessons learned
- [ ] A **final incident report** has been produced for management and board
- [ ] Results have been shared with **relevant stakeholders** (board, insurer, auditor)

Notes