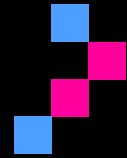


# Incident Response Quick Guide



*Initial*  
TECH

## **Purpose & how to use this quick guide**

Use this simple guide to coordinate a fast, consistent response to cyber incidents. It reflects common industry frameworks (SANS 6-step lifecycle; NIST SP 800-61 Rev.3 aligned to CSF 2.0; ISO/IEC 27035) and ACSC guidance for Australian organisations. Keep it short, actionable, and test it via tabletop exercises at least quarterly.

## 1. Key Roles & Contacts

Item	Notes
<b>Incident Manager:</b>	Leads response, decision-making, and comms; maintains this guide.
<b>Technical Lead:</b>	Coordinates investigation, containment, eradication, and recovery.
<b>Comms Lead:</b>	Handles internal/external communications; media; customer notices.
<b>Legal/Privacy:</b>	Advises on reporting obligations (e.g., OAIC, SOCI, GDPR/NIS2), evidence preservation.
<b>Vendor/MSP:</b>	Escalation to IR partners, cloud providers, backup vendors.

## 2. Severity & Initial Actions

Classify quickly and act within minutes. Example levels:

Item	Notes
<b>SEV1 (Critical):</b>	Widespread outage, ransomware deployment, confirmed data exfiltration – activate full IR team, isolate affected networks, engage vendors.
<b>SEV2 (Major):</b>	Multi-user compromise or targeted service impact – contain affected accounts/devices, increase monitoring, prepare external comms if customer impact.
<b>SEV3 (Minor):</b>	Single user/device or low impact – local containment and monitoring; document and review.

### 3. Incident Response Lifecycle (Quick Steps)

Item	Notes
<b>Preparation:</b>	Maintain plans, playbooks, logs/telemetry, backups, comms templates; train via tabletop exercises; define RACI roles.
<b>Identification:</b>	Confirm incident via alerts, logs, EDR/SIEM; capture initial facts (who/what/when/where); start an incident ticket and time-stamped log.
<b>Containment:</b>	Isolate affected hosts, accounts, and network segments; block IOCs; preserve evidence; protect backups (consider disconnecting online copies temporarily).
<b>Eradication:</b>	Remove malicious artefacts; patch and harden; rotate credentials; validate systems are clean.
<b>Recovery:</b>	Restore services systematically; monitor closely; verify with users; avoid re-infection; follow BCP/DR procedures.
<b>Lessons learned:</b>	Within 1–2 weeks, conduct review; update controls, playbooks, training; track actions to closure.

## 4. Ransomware – First 60 Minutes

Item	Notes
<b>Establish secure comms with IR team;</b> avoid email/IM on potentially compromised systems.	
<b>Rapid scoping:</b> identify impacted users/devices, originating device, payload, and command-and-control indicators.	
<b>Containment priority:</b> isolate affected endpoints; suspend suspected privileged accounts; stop remote sessions; block known IOCs; protect backups and consider temporary disconnection.	
<b>Evidence:</b> snapshot volatile data where safe; collect logs and timelines.	
<b>Decision:</b> invoke recovery strategy (clean restore or re-image) once eradication paths are ready; engage law enforcement/regulators as required.	

## 5. Communications Checklist

Item	Notes
Identify spokesperson and channels (email/SMS/status page).	
Prepare internal update: what is known/unknown, actions underway, how staff should report IOCs.	
Draft external customer notice (if applicable) with plain language and support steps.	
Coordinate regulatory notifications per jurisdiction (e.g., OAIC, SOCI timelines).	
Keep messages clear, consistent, and timely; avoid technical jargon when addressing non-technical audiences.	

## 6. Evidence & Reporting

Item	Notes
Maintain a time-stamped incident log (who, what, when).	
Preserve relevant artefacts (disk images, memory captures, logs) following chain-of-custody.	
Record containment/eradication steps, indicators blocked, accounts reset.	
Document regulatory notifications and law-enforcement references.	

## 7. Readiness Checklist (Quarterly)

Item	Notes
<b>Logging &amp; monitoring:</b> SIEM/EDR coverage verified; alerting thresholds reviewed.	
<b>Backups:</b> off-network immutable copy exists; periodic restore tests passed.	
<b>Access:</b> IR accounts with MFA; role-based permissions; break-glass procedure tested.	
<b>Playbooks:</b> phishing, credential compromise, ransomware, data breach updated.	
<b>Tabletop exercised;</b> actions tracked to closure.	

## References & Alignment

- SANS 6-step incident response lifecycle (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned).
- NIST SP 800-61 Rev.3 (2025) – incident response recommendations aligned to CSF 2.0 Functions (Govern, Identify, Protect, Detect, Respond, Recover).
- ISO/IEC 27035-1:2023 – principles and process for information security incident management.
- ACSC Cyber Incident Response Plan Guidance – template and readiness checklist for Australian organisations.
- CISA #StopRansomware – prevention best practices and response checklist.
- Microsoft Incident Response playbooks – ransomware approach and first-hour actions.