Incident Response Plan

Fillable template for Australian businesses | Version 1.0

Before you start

Complete this plan before an incident, not during one. Print a copy and store it somewhere that survives the incident itself - a plan saved only on an encrypted file server is not a plan. Review it every 12 months and after any incident or significant change to your systems, staff or obligations.

1. Organisation details

ORGANISATION / TRADING NAME

ABN

PLAN OWNER (NAME)

POSITION / ROLE

DATE THIS VERSION APPROVED

VERSION NUMBER

NEXT REVIEW DATE

DATE LAST TESTED / EXERCISED

2. Where this plan is kept

List every location. At least one must be reachable with no network, no email and no file server access.

PRIMARY LOCATION

OFFLINE / PRINTED COPY HELD BY

THIRD LOCATION (OPTIONAL)

3. Systems and data this plan covers

Name the systems that would trigger this plan if compromised - email, file storage, finance, client records, line-of-business applications, backups, and any system holding personal information.

Response team and contacts

Who does what, and how to reach them out of hours

4. Internal response team

Every role needs a named person and a named backup. If one person holds several roles, write their name in each.

ROLE	NAME	MOBILE (24/7)
Incident lead - decides and coordinates		
Deputy / backup lead		
Technical lead - containment and recovery		
Communications - clients and staff		
Legal / regulatory notifications		
Executive sponsor - authorises spend		

5. External contacts

Fill these in now. Looking up a phone number during an incident wastes the hours that matter most.

CONTACT	ORGANISATION AND NAME	PHONE
IT support / managed service provider		
Cyber insurance - insurer and policy number		
Insurer 24/7 incident hotline		
Legal adviser		
Accountant / bookkeeper		
Bank - fraud and disputed transactions		
Professional body / regulator contact		

> **Report cybercrime to ReportCyber at cyber.gov.au/report | Scamwatch: scamwatch.gov.au**
>
> If money has left an account, contact the receiving bank immediately - recovery windows are measured in hours.

6. Severity levels

Agree these definitions in advance so nobody has to argue about severity while an incident is running.

SEV 1	**Critical**	Business stopped, client data confirmed exposed, funds transferred, or systems encrypted.
SEV 2	**Major**	Significant disruption or suspected unauthorised access to sensitive data.
SEV 3	**Minor**	Contained, single user or system, no evidence of data access.

WHO CAN DECLARE A SEV 1, AND WHO MUST BE TOLD IMMEDIATELY

7. First response checklist

Tick as completed. Record the time against each - these timestamps matter for your notification obligations.

DONE	ACTION	TIME COMPLETED
☐	Record the date and time the incident was first noticed, and by whom	
☐	Do not turn affected machines off - disconnect from the network instead, preserving evidence	
☐	Contact the incident lead and IT support	
☐	Isolate affected accounts: reset passwords, revoke sessions, disable compromised logins	
☐	Check whether any payment or bank detail changes were made or requested	
☐	Identify what data may have been accessed, and whose	
☐	Notify your insurer before engaging any third-party responder - cover can depend on it	
☐	Start the incident log on page 5 and keep it contemporaneous	
☐	Do not pay any ransom or extortion demand without legal advice and sanctions screening	

Notification obligations

Overlapping clocks - check each one against the facts

These obligations run in parallel, not in sequence.

A single incident can trigger several at once, each with a different trigger and a different deadline.

8. Obligation checklist

- [ ] **Notifiable Data Breaches scheme (OAIC)**
  Trigger: Personal information accessed, disclosed or lost, and likely to result in serious harm.
  Deadline: As soon as practicable. Maximum 30 days to assess.
  NOTIFIED (DATE / TIME)

- [ ] **Ransomware / cyber extortion payment report**
  Trigger: A payment was made, or made on your behalf. Applies at $3m+ turnover.
  Deadline: 72 hours from payment or from becoming aware of it.
  NOTIFIED (DATE / TIME)

- [ ] **Affected individuals**
  Trigger: Required where the breach is an eligible data breach under the NDB scheme.
  Deadline: As soon as practicable after determining.
  NOTIFIED (DATE / TIME)

- [ ] **Clients and business partners**
  Trigger: Their data, matters or funds are affected, or contracts require it.
  Deadline: Per contract. Check engagement terms.
  NOTIFIED (DATE / TIME)

- [ ] **Cyber insurer**
  Trigger: Almost always required immediately, and before engaging responders.
  Deadline: Immediately. Check policy wording.
  NOTIFIED (DATE / TIME)

- [ ] **Industry regulator or professional body**
  Trigger: Sector obligations - e.g. AUSTRAC, ATO, TPB, law society, APRA, ASIC.
  Deadline: Varies. Record which applies to you.
  NOTIFIED (DATE / TIME)

- [ ] **Police / ReportCyber**
  Trigger: Criminal conduct, fraud, extortion or theft of funds.
  Deadline: As soon as possible.
  NOTIFIED (DATE / TIME)

OTHER OBLIGATIONS SPECIFIC TO THIS ORGANISATION

Incident log

Keep this contemporaneous - write it down as it happens

A contemporaneous log is the single most useful document you will have afterwards. It shapes what you must notify, supports your insurance claim, and demonstrates that you acted reasonably. Record decisions and the reasons for them.

INCIDENT REFERENCE	SEVERITY	DATE OPENED

DATE / TIME	WHO	WHAT HAPPENED / WHAT WAS DECIDED

Post-incident review

The step almost everyone skips

9. What happened

10. How it was detected, and how long that took

11. What worked, and what did not

12. Actions to prevent recurrence

ACTION	OWNER	DUE DATE

REVIEW COMPLETED BY	DATE OF REVIEW	PLAN UPDATED? (Y/N)

Need help closing the gaps this review identified?

Mobile Techs IT Consulting supports Gold Coast businesses on-site and firms across Australia remotely.
1300 644 588 | office@mobiletechs.com.au | mobiletechs.com.au