



OMNICON
I.T. SERVICES

POLICIES & PROCEDURES · TEMPLATE

Cyber Incident Response Plan Template

Plan who does what if your business experiences a cyber incident, using a clear six-step sequence from identification to review.

Who this is for

Small businesses that want a written plan for what to do if they experience a cyber incident, such as ransomware, a compromised email account or a data breach.

How to use it

- Complete the plan now, while things are calm. Fill in contacts and critical systems before you need them.
- Keep a printed copy somewhere that does not depend on your computers or email.
- Review the plan every year and after any incident or major change.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.

The six-step response sequence

When something goes wrong, follow these steps in order. Work through the detailed sections that follow for each step.

1 Identify Recognise that something is wrong and record what you see.	2 Assess Decide how serious it is and what is affected.	3 Contain Limit the damage without destroying evidence.	4 Escalate Bring in the right people and professional help.	5 Recover Restore systems safely from trusted sources.	6 Review Learn from it and improve your defences.
---	---	---	---	--	---

Ransomware or a suspected compromise needs immediate professional help

If files are being encrypted, you see a ransom note, or an attacker may have access to your systems, contact your IT provider immediately. **Do not** pay or negotiate with attackers, delete files or logs, wipe devices, or reconnect affected systems until they have been assessed by a professional.

1. Business details

Business name	ABN
Main address	Plan owner
Plan version	Date last reviewed

2. Incident coordinator

The coordinator leads the response, makes decisions and keeps the incident log. Name a backup in case they are unavailable.

Role	Name	Phone	Alternative contact
Incident coordinator			
Backup coordinator			

3. Contacts

Internal contacts

Role	Name	Phone	Responsibility in an incident
Owner or director			
Finance			
Operations			

Role	Name	Phone	Responsibility in an incident

External contacts

Organisation	Contact name	Phone	Account or policy number
IT support provider			
Cyber insurer			
Bank			
Legal adviser			
Internet provider			
Key software supplier			

To report cybercrime in Australia, use ReportCyber at cyber.gov.au or call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371). In an emergency or if someone is in danger, call 000.

4. Critical systems

List the systems your business cannot operate without, and how long you could cope without each.

System or data	Used for	Supplier or location	Owner	Maximum outage

Step 1: Identify

Common signs of an incident include unexpected account lockouts, unusual sign-in alerts, emails sent that staff did not write, files that will not open or have changed names, ransom messages, and unexpected payment changes.

Date and time noticed

Noticed by

What was observed

Systems or accounts involved

Step 2: Assess the initial severity

Severity	What it looks like	Response
Low	A single suspicious email that was not clicked, or a blocked malware alert.	Record it, report it and monitor.
Medium	One account or device may be affected, but business operations continue.	Contain the affected account or device and contact IT support the same day.
High	Several accounts or systems are affected, data may have been accessed, or payments are at risk.	Escalate immediately to the coordinator and IT support.
Critical	Ransomware, widespread compromise or a business-stopping outage.	Contact IT support and your insurer immediately. Follow their instructions.

Assessed severity

Assessed by and time

Step 3: Contain

Containment priorities, guided by your IT provider:

- Disconnect an affected device from the network (unplug the network cable or turn off Wi-Fi). **Do not turn it off or wipe it** unless your IT provider advises you to, because this can destroy evidence.
- Reset passwords for affected accounts from a known-safe device, and sign out other sessions.
- Contact your bank immediately if payments or banking details may be affected.
- Protect your backups: disconnect backup drives and stop any scheduled jobs that could overwrite good backups.

Preserve evidence

- Write down everything you see, with times, in an incident log.
- Take photos or screenshots of ransom notes, error messages and suspicious emails.
- Keep suspicious emails. Do not delete them, forward them to colleagues or click anything in them.
- Do not delete logs, files or accounts.

Step 4: Escalate

Done	Action	Time	By whom
☐	Incident coordinator informed		
☐	IT support provider contacted		
☐	Cyber insurer notified (check your policy's notification timeframe)		

Done	Action	Time	By whom
☐	Bank contacted, if payments may be affected		
☐	Legal adviser consulted, if personal or sensitive data may be involved		
☐	Incident reported to ReportCyber, where appropriate		

Legal, regulatory and contractual considerations

Depending on your business and the incident, you may have obligations to notify others. Seek legal advice if you are unsure.

- **Privacy:** if personal information may have been accessed and the Notifiable Data Breaches scheme applies to you, you may need to assess the breach and notify affected individuals and the OAIC.
- **Contracts:** customer, supplier or government contracts may require you to report incidents within a set time.
- **Insurance:** most cyber policies require prompt notification, and some require you to use approved responders.
- **Industry rules:** some sectors have their own reporting requirements.

Step 5: Recover

- Only reconnect or restore systems once they have been assessed and cleaned or rebuilt.
- Restore data from a backup taken before the incident began, and check it is complete.
- Change passwords and review MFA methods on affected accounts.
- Monitor closely for signs the problem has returned.

Communications responsibilities

Audience	Who communicates	What and when
Staff		
Customers		
Suppliers and partners		
Media and public		

Step 6: Post-incident review

Date of review

Attendees

What happened, and when was it detected?

What worked well in our response?

What would we do differently?

Lessons learned and improvements

Improvement	Owner	Target date	Done

Incident log

Date and time	What happened or action taken	By whom

Date and time	What happened or action taken	By whom

Need a hand?

Omnicon I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.