JCPIT | SUPPORT
KEEPING IT SIMPLE

INCIDENT RESPONSE CHECKLIST

Cyber incident first hour.

A calm, practical sequence for contacting help, containing harm and preserving evidence.

PREPARED BY
JCPIT Support Pty Ltd

USE THIS COPY
Owner: _____ Edition: July 2026

STAY CALM AND PRESERVE OPTIONS

The first 30 minutes

CHECKLIST · 01

Use a printed or offline copy. If business email may be compromised, coordinate through a separate trusted channel.

BUSINESS	INCIDENT RESPONSE LEAD
IT / SECURITY PROVIDER PHONE	CYBER INSURER / POLICY NUMBER
SAFE COMMUNICATION CHANNEL	INCIDENT START TIME

01

PRIORITISED FIRST STEP

Call your incident contact using a trusted number.

State what happened, when it started and who or what is affected. Check the insurer's incident instructions early because approval requirements may apply.

0–10 Activate the response

- [ ] Record the time, reporter, affected account or device, and the first visible symptom.
- [ ] Contact the IT or security provider using a known phone number, not details in a suspicious message.
- [ ] Check the cyber insurance policy and contact the approved response service when required.
- [ ] Move coordination away from business email if an attacker may be reading it.

INCIDENT LEAD _____ INCIDENT LOG LOCATION _____

10–30 Contain on advice

- [ ] Follow instructions to isolate affected devices or disable affected accounts.
- [ ] If damage is clearly spreading and help is unavailable, disconnect the device's network cable or Wi-Fi.
- [ ] Leave the device powered on unless an incident responder tells you otherwise.
- [ ] Stop using an affected device for password changes, banking or sensitive communication.

TECHNICAL LEAD _____ ACTIONS AND TIMES _____

SCOPE, PRESERVE, COMMUNICATE

Minutes 30 to 60

30–45 Preserve useful records

- [ ] Photograph unusual screens or messages if it is safe to do so.
- [ ] Keep suspicious emails and files. Do not forward them widely.
- [ ] Record every action, who approved it and the exact time.
- [ ] List affected people, devices, accounts, files and business services.

EVIDENCE OWNER _____

PROTECTED EVIDENCE LOCATION _____

45–60 Issue a factual update

- [ ] State the status: Investigating, Contained, Active or Resolved.
- [ ] Write what is known, what is not yet known and what staff must avoid.
- [ ] Set the next update time, even if there may be no new finding.
- [ ] Name where staff should report new symptoms using a safe channel.

COMMUNICATION OWNER _____

NEXT UPDATE BY _____

Do not make the incident harder to investigate

- Do not install cleanup tools, delete files, reset equipment or restore backups without advice.
- Do not pay a ransom or contact an attacker before speaking with incident, legal and insurance advisers.
- Do not make public statements based on guesses or name the staff member who reported the issue.
- Do not assume notification requirements. Get privacy or legal advice if personal information may be involved.

FIRST-HOUR STATUS

CURRENT STATUS	BUSINESS IMPACT	NEXT UPDATE TIME

A SECOND SET OF EYES

Prepare before an incident.

Current JCPIT clients should use their agreed incident contact. The public number is not a promise of 24 × 7 response. Before an incident, book a Free Security Check to review accounts, backups and response contacts.

jcpit.com.au/free-security-check/
(03) 9021 0890

Preparation matters: keep trusted phone numbers, insurer details and this checklist available when email is not. Store the completed checklist securely. Do not record passwords, authentication codes, full bank details or unnecessary personal information. Share it only with authorised response, legal and insurance contacts.