Good Security

TEMPLATE WATERMARKED PDF

WORKING TEMPLATE

Incident Response Plan Template

A complete incident response plan template for NZ SMEs, covering detection through post-incident review. Aligned to CERT NZ guidance and Privacy Act 2020 notification obligations.

Branded customer-ready document | Shareable with leadership teams | Generated 12 Mar 2026

For New Zealand small and medium-sized businesses

Good Security · goodsecurity.co.nz · **hello@goodsecurity.co.nz**

> **How to use this template** Customise every section marked [IN SQUARE BRACKETS] for your organisation. Remove this instruction box before finalising. Review and test this plan at least annually — and after any significant incident or major change to your business. The best time to read your incident response plan is not during an incident.

Organisation: _____ **Plan version:** 1.0 **Last reviewed:** _____
Plan owner: _____

SECTION 1: PURPOSE AND SCOPE

This Incident Response Plan defines how [ORGANISATION NAME] will detect, respond to, contain, and recover from cybersecurity incidents. It applies to all staff, contractors, and systems that store, process, or transmit business or personal information.

This plan is aligned to CERT NZ guidance for NZ businesses and the requirements of the Privacy Act 2020, including mandatory reporting obligations for notifiable privacy breaches.

SECTION 2: INCIDENT RESPONSE TEAM

Primary contacts

ROLE	NAME	PHONE	EMAIL
Incident Response Lead	[NAME]	[PHONE]	[EMAIL]
Backup / Deputy	[NAME]	[PHONE]	[EMAIL]
IT / Technical contact	[NAME / PROVIDER]	[PHONE]	[EMAIL]
Legal / Privacy advisor	[NAME / FIRM]	[PHONE]	[EMAIL]
Senior management	[NAME]	[PHONE]	[EMAIL]

External contacts

ORGANISATION	CONTACT	PHONE / URL
CERT NZ	Incident reporting	0800 CERT NZ · cert.govt.nz
Office of the Privacy Commissioner	Breach notification	privacy.org.nz
NZ Police (if criminal activity)	Non-emergency line	105
Cyber insurance provider	[PROVIDER NAME]	[PHONE / EMAIL]
IT managed service provider	[MSP NAME]	[PHONE]

SECTION 3: WHAT COUNTS AS A CYBERSECURITY INCIDENT?

A cybersecurity incident is any event that compromises — or could compromise — the confidentiality, integrity, or availability of your systems or information.

Account compromise

- A staff account is accessed without authorisation
- Login alerts from unfamiliar locations or devices
- Unusual email forwarding rules discovered

Malware / ransomware

- Files have been encrypted and a ransom is demanded
- Antivirus detects and quarantines malware

- A device is behaving abnormally — slow, unexpected processes, unusual network activity

Phishing

- A staff member clicked a link in a phishing email
- Credentials were entered on a fake login page
- Money or gift cards were sent in response to a fraudulent email (Business Email Compromise)

Data breach / exfiltration

- Personal or confidential information was accessed by an unauthorised party
- A device containing sensitive information was lost or stolen
- Personal data was accidentally sent to the wrong recipient

System compromise

- Unauthorised access to a server, database, or business application
- Website defacement or takeover
- Evidence of an attacker moving laterally through your environment

Denial of service

- A business-critical system or website becomes unavailable
- Email stops working

SECTION 4: INCIDENT SEVERITY LEVELS

🔴 Critical — immediate response required

- Active ransomware encryption in progress
- Confirmed data breach affecting a large number of individuals or highly sensitive data
- Complete loss of access to critical business systems
- Evidence of an active attacker inside your network

Response time: Immediately. Call the Incident Response Lead now. Do not wait.

🟠 High — response within 2 hours

- Suspected account compromise of an administrator or executive
- Ransomware detected but not yet spreading
- Loss or theft of an unencrypted device containing sensitive data
- Phishing email confirmed actioned — credentials entered or payment made

Response time: Within 2 hours.

🟡 Medium — response within business day

- Phishing email clicked but no credentials entered or actions taken
- Malware quarantined by antivirus software
- Suspicious activity detected but not yet confirmed as compromise
- Privacy breach affecting a small number of individuals

Response time: Within the same business day.

🟢 Low — monitor and log

- Phishing email received but not acted on
- Failed login attempts on a non-privileged account
- Minor policy violations with no security impact

Response time: Log and review. Escalate if a pattern emerges.

SECTION 5: INCIDENT RESPONSE PHASES

PHASE 1: DETECT & REPORT

Goal: Identify that an incident has occurred and get the right people involved.

1. Any staff member who suspects or discovers an incident contacts the Incident Response Lead immediately using the contacts in Section 2.
2. Do not attempt to investigate or fix the problem yourself unless instructed.
3. Do not turn off or restart affected devices — this destroys forensic evidence.
4. Do not discuss the incident on affected systems — avoid email or Teams/Slack on compromised environments. Use phone or a separate, unaffected device.
5. The Incident Response Lead assesses severity and activates the appropriate response level.

□ Incident identified and Incident Response Lead notified □ Severity level assessed □ Affected systems identified (do not touch yet) □ Initial notes documented — what was seen, when, on which device

Staff reporting: All staff should know they can report a suspected incident to [PHONE/EMAIL] without fear of blame. Incidents reported early are far easier to contain.

PHASE 2: CONTAIN

Goal: Stop the incident from spreading or causing further damage.

For account compromise: □ Immediately reset passwords for compromised accounts □ Revoke active sessions (Microsoft 365: sign out all sessions via admin portal) □ Review and remove any malicious email forwarding rules □ Disable compromised accounts if necessary □ Check whether the compromised account accessed other systems

For malware / ransomware: □ Isolate affected devices from the network immediately — disconnect ethernet, disable Wi-Fi. Do not turn off the device. □ Identify the scope: which devices and file shares are affected? □ Notify your IT provider immediately □ Do not pay any ransom without legal and insurance advice

For device loss or theft: □ Consider remote wipe if enabled — note this will destroy forensic evidence; discuss with IR Lead first □ Revoke access credentials that were accessible on the device □ Identify what data was on the device

For data breach: □ Stop ongoing access or exfiltration where possible □ Preserve logs and evidence □ Do not delete or modify affected systems

---

PHASE 3: ASSESS & INVESTIGATE

Goal: Understand what happened, what data was affected, and the full scope of the incident.

1. Work with your IT provider or Good Security to investigate the incident.
2. Preserve and collect evidence: logs, screenshots, email headers, affected files. Maintain a chain of custody.
3. Determine: What systems were accessed? What data was accessed or exfiltrated? How did the attacker gain access? What is the full timeline?
4. Assess Privacy Act obligations: Was personal information accessed? How many individuals are affected? How sensitive is the data?

Key questions to answer:

- How did the attacker get in? (Phishing, credential stuffing, unpatched vulnerability, insider?)
- What did they access or take?
- Is the attacker still inside the environment?
- What is the complete list of affected individuals and data?

PHASE 4: NOTIFY

Goal: Meet legal notification obligations and communicate appropriately.

Privacy Commissioner notification

Under the Privacy Act 2020, you **must** notify the Privacy Commissioner if the breach has caused, or is **likely to cause**, serious harm. Notification must occur **as soon as practicable** after you become aware.

Notify at: privacy.org.nz (search "notify a privacy breach")

Information required for notification:

- Name and contact details of your organisation
- Description of what happened
- What personal information was involved
- How many individuals are affected
- What steps have been taken to contain the breach
- Whether affected individuals have been notified

Affected individual notification

Notify affected individuals if the breach poses a real risk of harm — financial fraud, identity theft, or safety risk. Notifications must:

- Be clear and in plain English
- Explain what happened and what information was involved
- Describe what you are doing about it
- Advise what individuals can do to protect themselves
- Provide a contact for questions

Cyber insurance

Notify your cyber insurer as soon as possible. Most policies require prompt notification and have specific claims procedures. Legal and forensic costs are often covered.

Other notifications

Depending on the nature of the incident:

- Your bank — if financial fraud is involved
- CERT NZ — cert.govt.nz — to help protect other NZ businesses
- NZ Police — if criminal activity is involved
- Affected business partners or suppliers

PHASE 5: ERADICATE & RECOVER

Goal: Remove the threat and restore systems securely.

1. Remove malware, close attacker access, and patch the vulnerability that was exploited.

2. Restore from clean backups where systems were compromised.
3. Verify backups are clean before restoring — ransomware can corrupt backup files.
4. Reset credentials for all potentially affected accounts.
5. Rebuild compromised systems from known-good images where possible.
6. Test systems before returning to production.
7. Implement additional controls to prevent recurrence.

□ Threat removed and attacker access closed □ Systems restored from clean backup □ Credentials reset across affected accounts □ Systems tested before returning to production □ Additional controls implemented

---

PHASE 6: REVIEW

Goal: Learn from the incident to strengthen your security.

Complete within 2 weeks of resolution:

1. Conduct a post-incident review with all relevant staff.
2. Document: what happened, timeline, root cause, containment actions, and recovery steps.
3. Identify what controls failed or were absent.
4. Create an action plan to address identified weaknesses.
5. Update this plan if gaps were identified.
6. Consider whether additional staff training is required.

Post-incident review questions:

- What was the root cause?
- Could it have been detected sooner? What would have helped?
- Was the response effective? What took longer than expected?
- What controls would have prevented this incident?
- Are there other systems or processes with similar vulnerabilities?

SECTION 6: INCIDENT LOG

Maintain a written log of all incidents, including low-severity events. This creates a pattern record and supports compliance obligations.

DATE	DESCRIPTION	SEVERITY	ACTIONS TAKEN	OUTCOME	NOTIFIED?

SECTION 7: PLAN MAINTENANCE

This plan must be reviewed:

- Annually as a minimum
- After any significant incident
- After major changes to the business, systems, or staff

Next scheduled review: _____

Plan tested (tabletop exercise): _____

QUICK REFERENCE CARD

Print this page and keep it accessible offline — do not rely on systems that may be compromised.

INCIDENT HOTLINE: [PHONE]

CERT NZ: 0800 CERT NZ · cert.govt.nz

Privacy Commissioner: privacy.org.nz

Cyber insurer: [PROVIDER] — [PHONE]

IMMEDIATE STEPS IF YOU SUSPECT AN INCIDENT:

1. Don't panic. Don't touch anything unless told to.
2. Call [INCIDENT RESPONSE LEAD NAME] on [PHONE].
3. If you can't reach them, call [BACKUP] on [PHONE].
4. Don't discuss on email or Teams — use your phone.
5. Write down what you saw, when, and on which device.