POLICY DOCUMENT

Cyber Incident

Response Plan

Organisation: [Organisation Name]
Version: 1.0
Effective Date: [Date]
Review Date: [Date + 12 months]
Policy Owner: [Name / Role]

Prepared by [IT Provider Name]

IMPORTANT — KEEP ACCESSIBLE OFFLINE
This document contains sensitive information about the organisation's security response procedures. A printed copy must be held by the Incident Commander and stored in a location accessible if IT systems are unavailable.

---

1. Purpose

This Cyber Incident Response Plan establishes the procedures [Organisation Name] will follow when a cyber security incident occurs or is suspected. Its objectives are to detect and confirm incidents quickly, contain and eradicate their cause, restore normal operations, meet obligations under the Privacy Act 2020, preserve evidence, and learn from incidents to improve the organisation's security posture.

---

2. Scope

This Plan applies to all cyber security incidents including ransomware and malware, phishing and business email compromise, unauthorised access to systems or data, data breaches involving personal information, denial of service attacks, insider threats, supply chain compromises, and loss or theft of devices containing organisational data.

---

3. Incident Severity Classification

Level	Classification	Description	Response Time
P1	Critical	Active ransomware, confirmed data breach, complete system outage, active intrusion	Immediate — within 1 hour
P2	High	Suspected breach, significant malware, compromised admin credentials, major disruption	Within 4 hours
P3	Medium	Phishing email clicked, single device infected, suspicious activity, minor data exposure	Within 24 hours
P4	Low	Policy violation, unsuccessful attack, lost device with no data	Within 5 business days

---

4. Incident Response Team

Role	Name	Mobile	Alternate
Incident Commander	[Name]	[Mobile]	[Alternate]
IT Lead — [IT Provider Name]	[Name]	[IT Provider Phone]	[Alternate]
Communications Lead	[Name]	[Mobile]	[Alternate]
Privacy Officer / Legal	[Name]	[Mobile]	[Alternate]
Senior Management	[Name]	[Mobile]	[Alternate]

---

5. Response Phases

Phase 1 — Detection and Reporting

1. Stop using the affected system immediately — do not attempt to fix the issue yourself
2. Do not turn off the device unless instructed — powered systems preserve evidence
3. Note the time, what you observed, and any actions taken before reporting
4. Contact [IT Manager / IT Provider] immediately on [IT Provider Phone]
5. Do not discuss the incident on email or messaging systems that may be compromised — use phone

AFTER HOURS INCIDENTS
For P1 or P2 incidents outside business hours, contact [IT Provider Name] on [IT Provider Phone].

Do not wait until the next business day to report a suspected ransomware infection or active breach.

Phase 2 — Assessment and Classification

The IT Lead will assess the incident and assign a P1 to P4 severity classification, determining the nature and scope of the incident, which systems and data are affected, whether personal information has been compromised, whether the incident is ongoing, and whether external assistance is required.

Phase 3 — Containment

Containment actions may include isolating affected devices from the network, blocking compromised user accounts, taking affected systems offline, blocking malicious IP addresses or domains at the firewall, and suspending access for third-party providers whose systems may be involved.

Phase 4 — Eradication

The cause of the incident must be identified and removed. Malware must be removed from all affected systems, compromised credentials revoked and replaced, vulnerabilities remediated, and affected systems scanned and verified clean before restoration.

Phase 5 — Recovery

Systems will be restored from clean verified backups, in priority order starting with the most critical functions, with close monitoring for reinfection, and with confirmation from business units before closing the incident.

Phase 6 — Post-Incident Review

Within 10 business days of resolution, the Incident Commander will convene a review to document a timeline, identify the root cause, assess the effectiveness of the response, and identify improvements. A Post-Incident Report must be completed and retained for at least three years.

---

6. Communication

Internal Communication

The Incident Commander will determine what information is shared with staff and when. Staff must not discuss the incident publicly until authorised to do so.

External Communication

All external communications — including to clients, media, or regulators — must be approved by Senior Management before being sent.

Regulatory Notification

Where the incident has resulted in or may have resulted in a privacy breach involving personal information, the organisation must assess whether it constitutes a notifiable privacy breach under the Privacy Act 2020. A breach is notifiable if it is likely to cause serious harm to any affected individual.

- Notification to the Office of the Privacy Commissioner must be made as soon as practicable
- Notification to affected individuals must be made as soon as practicable

OFFICE OF THE PRIVACY COMMISSIONER

Notifiable breach notifications must be submitted at privacy.org.nz/your-rights/notifiable-privacy-breaches/ or by calling 0800 803 909. Seek legal advice before making any public statements about a breach.

---

7. Ransomware — Specific Guidance

6. Disconnect affected devices from the network immediately — remove network cables, disable Wi-Fi
7. Do not turn off affected devices unless instructed — memory forensics may be possible
8. Contact [IT Provider Name] immediately on [IT Provider Phone]
9. Do not pay any ransom without taking legal and expert advice
10. Identify the most recent clean backup and verify its integrity
11. Notify Senior Management and the Incident Commander immediately

RANSOM PAYMENT

Any decision to pay must be made by Senior Management with legal advice. Payment does not guarantee data recovery, may fund criminal activity, and may have legal implications under New Zealand law.

---

8. Backup and Recovery

System / Data	Backup Frequency	Retention	Location
Microsoft 365	Daily	30 days	Veeam for M365
[System Name]	[Frequency]	[Retention]	[Location]
[System Name]	[Frequency]	[Retention]	[Location]

Backups must be tested at least quarterly. At least one backup copy must be offline or in an immutable cloud location, separate from the primary environment.

9. Plan Testing

This Plan must be tested at least annually through a tabletop exercise or simulated incident to verify contact details are current, staff understand their roles, backup and recovery procedures work, and gaps are identified and addressed. [IT Manager / IT Provider] will facilitate annual testing.

10. Related Documents

- Acceptable Use Policy
- Artificial Intelligence Acceptable Use Policy
- Business Continuity Policy
- Privacy Breach Response Procedure

Acknowledgement

I confirm that I have read and understood the Cyber Incident Response Plan and my responsibilities within it.

Full Name

Role

Signature

Date

Document Control

Version	Date	Author	Summary of Changes
1.0	[Date]	[IT Provider Name]	Initial version

Prepared by [IT Provider Name] | [IT Provider Website] | [IT Provider Phone]