



Cyber Incident Response Policy

SMB1001 Control 22 · pairs with the Emergency Action Card.

Is an incident happening now? Stop reading and follow the *Shit, We've Actually Been Hacked!* Emergency Action Card.

This policy explains who is responsible, who can make decisions and how our business prepares for and learns from cyber incidents. The Emergency Action Card contains the immediate response steps and forms part of this policy.

1. Purpose

Our business will respond quickly, calmly and responsibly to suspected cyber incidents. Our priorities are to protect people and money, contain the incident, preserve evidence, restore operations safely and meet our legal, contractual and insurance obligations.

2. Who and what this covers

This policy applies to all employees, contractors, devices, accounts, systems, cloud services and business information. A cyber incident may include a hacked account, suspicious MFA prompt, malware or ransomware, payment fraud, lost device, exposed information or unexpected system outage. Anyone who suspects an incident must report it immediately and follow the Emergency Action Card. Proof is not required, and nobody will be blamed for reporting a genuine concern.

3. Responsibilities and authority

Everyone must:

- report suspected incidents immediately
- stop using an affected device or account
- follow the Emergency Action Card
- preserve messages, files and other potential evidence
- avoid discussing the incident externally unless authorised.

The incident decision-maker or deputy will:

- coordinate the business response
- contact the IT provider and cyber insurer
- authorise major operational, financial and communication decisions
- determine what external notifications are required
- decide when normal operations can resume.

The IT provider / MSP will:

- advise on containment, investigation and recovery
- preserve relevant technical evidence where possible
- confirm when systems and backups are safe to use
- take reasonable, reversible containment action where authorised and necessary to prevent further harm.

The decision-maker and deputy are named on the Emergency Action Card.

4. Response rules

During an incident:

- affected systems will be contained as quickly and safely as possible
- important actions and decisions will be recorded
- backups will not be connected or restored until the IT provider confirms it is safe
- potentially compromised email or messaging will not be used to coordinate the response
- only authorised people may communicate with customers, suppliers, the media or the attacker
- our default position is not to pay a ransom or extortion demand.

Any decision involving a ransom or extortion payment requires the decision-maker's approval after insurer, legal and government advice and consideration of applicable reporting and sanctions obligations.

5. Notifications and communications

The decision-maker will obtain appropriate advice and determine whether the incident must be reported to:

- the cyber insurer
- the bank or payment provider
- ASD's Australian Cyber Security Centre
- the OAIC and affected individuals
- police or another regulator
- affected customers, suppliers or contractual partners.

Notifications will be accurate, timely and limited to verified information. Other staff must refer external questions to the decision-maker.

6. Recovery and improvement

Systems will only return to operation after the IT provider confirms that the threat has been contained and recovery is safe. Following a significant incident, the business will hold a short review to determine:

- what happened and what was affected
- what worked and what caused delays
- what must be changed
- who is responsible for completing each improvement.

An incident record will be stored securely.

7. Keeping this policy ready

The business will:

- keep the Emergency Action Card completed, printed and accessible
- show every worker where it is and how to use it
- confirm emergency contacts and backup access at least annually
- test the policy and Emergency Action Card at least annually
- review them after an incident or significant change to the business, systems, insurer or IT provider.

Sign-off

Business: _____

Policy owner: _____

Approved by: _____

Date: _____

Last tested: _____

Next review: _____

Related document: *Shit, We've Actually Been Hacked! Emergency Action Card*

DI(m)Y™ · Do It (mostly) Yourself · www.steady-point.com · Free to use and adapt to your business. General information, not legal advice.