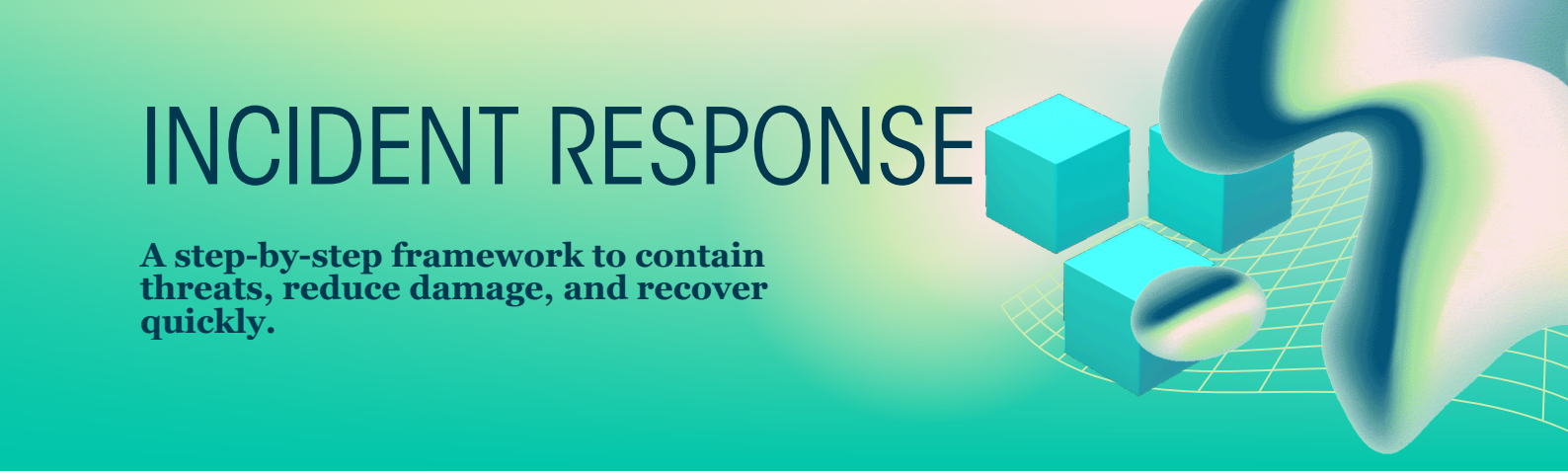

Incident Response Plan Template for Small Businesses (2026 Edition)

This template gives your business a simple, repeatable plan to follow under pressure.

SECTION 1 — Business Information (Fill This Out First)

Company Name: _____
Primary Contact: _____
IT Provider / Support Contact: _____
Emergency Phone: _____

Critical Systems (check all that apply):
☐ Email
☐ File Storage
☐ Accounting Software
☐ CRM
☐ Website
☐ Payment Systems

SECTION 2 — Incident Identification

What happened? (Check one or more)
☐ Suspicious email or phishing attempt
☐ Account login alert or unauthorized access
☐ Malware or ransomware detected
☐ Lost or stolen device

□ System outage or unusual behavior
□ Data breach or data exposure

Date/Time Detected: _____
Who reported it: _____

Initial Observations:

SECTION 3 — Immediate Response Actions (First 15–30 Minutes)

□ Do NOT click links, download files, or respond to attackers
□ Disconnect affected device from internet (Wi-Fi off / unplug cable)
□ Secure compromised accounts (change passwords immediately)
□ Enable or verify MFA on affected accounts
□ Notify internal contact or IT support immediately

Why this matters:
Fast containment prevents spread. Most damage happens after the first mistake.

SECTION 4 — Containment Checklist

□ Identify all affected users/devices
□ Disable compromised accounts temporarily
□ Block suspicious IP addresses or domains (if possible)
□ Remove malicious emails from inboxes (company-wide if needed)
□ Isolate infected systems from the network

Notes:

SECTION 5 — Assessment & Impact

What systems are affected?

What data may be at risk?
□ Emails
□ Customer data
□ Financial data
□ Login credentials
□ Internal documents

Business Impact Level:
□ Low (minor disruption)

□ Medium (partial downtime or risk exposure)
□ High (data breach, full outage, or financial risk)

SECTION 6 — Communication Plan

Internal Notification:
□ Inform team members of the issue
□ Provide clear instructions (do NOT speculate)

External Notification (if required):
□ Customers
□ Vendors
□ Legal/compliance contacts

Key Rule:
Only one person communicates externally to avoid confusion.

SECTION 7 — Recovery Actions

□ Restore systems from verified backups
□ Reinstall or clean infected devices
□ Reset all affected passwords
□ Reconnect systems only after verification
□ Monitor for repeat activity

Why this matters:
Restoring too early can reinfect your systems.

SECTION 8 — Post-Incident Review (Within 48 Hours)

□ What caused the incident?
□ What worked in the response?
□ What failed or slowed us down?
□ What needs to change immediately?

Action Items:

SECTION 9 — Prevention Checklist (After the Incident)

◻ Enable MFA across all systems
◻ Implement password manager for team access
◻ Verify backup systems and test recovery
◻ Provide employee phishing/security training
◻ Update software and patch systems

Why this matters:
Prevention is less expensive than recovery.

SECTION 10 — Emergency Contacts Sheet

IT Support / MSP: _____
Email Provider Support: _____
Bank / Financial Contact: _____
Legal / Compliance Contact: _____

Keep this section accessible even if systems are down.

Quick Response Flow (Print This Section)

1. **Identify the issue**
2. **Disconnect affected systems**
3. **Secure accounts**
4. **Notify IT support**
5. **Contain the spread**
6. **Assess damage**
7. **Recover safely**
8. **Review and improve**

Rule of Thumb

Delays increase damage.
Clear actions reduce it.