CICADA | RESOURCES

RESPONSE | 45 MIN | ESSENTIAL | UPDATED NOVEMBER 2026

Write a one-page incident plan

Names, numbers and the first hour. Not a 40-page policy nobody can find at 8am.

The short version

- ✓ One page, printed, available offline.
- ✓ Name a decision-maker and a deputy.
- ✓ Include bank, insurer, IT and legal contacts.
- ✓ Rehearse it once a year with the people named.

What belongs on the page

- **Decision-maker and deputy**: who can authorise payments, shutdowns and public statements.
- **Contacts**: bank fraud line, insurer incident line, IT provider, legal, landlord, key suppliers.
- **First hour steps**: isolate, call, preserve, communicate.
- **Do-not list**: don't pay, don't wipe, don't email the attacker, don't speculate publicly.
- **Log**: time, action, who decided.

Test it before you need it

Book 45 minutes with the people named. Read through a scenario: “The bookkeeper's laptop shows a ransomware note and files on the shared drive won't open.” Walk the page. Who calls the bank? Who calls the insurer? Who tells staff? What's the order?

You'll find at least two gaps: a wrong number, a missing role, a supplier nobody can reach. Fix them.

Keep it current

Review every six months and after any change of staff, bank or insurer. Print two copies: one in the office, one with the owner. Store a copy offline in case email and file storage are unavailable.

> **USE THE TEMPLATE**
>
> Our printable incident card has the structure ready. Fill in the blanks and keep it with your backup plan.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] Decision-maker and deputy named
- [ ] Bank, insurer, IT and legal contacts verified
- [ ] First-hour steps written
- [ ] Do-not list included
- [ ] Two printed copies stored offline
- [ ] Annual walkthrough booked

0 of 6 done