Incident response plan template for small business

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

1. Prepare: who is in charge

Write this page once and print it.

- Incident lead: [name], phone [number]. Deputy: [name], phone [number].
- Outside help: [IT provider or incident response firm], phone [number]. Insurance hotline: [number], policy [number].
- Where the backups are and who can restore them: [location and name]. Test a restore once a year.
- The three systems we cannot run without: [system 1], [system 2], [system 3].

2. Identify: what counts as an incident

Call the incident lead if any of these happen.

- Someone clicked a link or opened a file and the device now behaves oddly.
- A password or account was shared, guessed or used by someone else.
- A device with business data is lost or stolen.
- A payment request or bank detail change looks wrong.
- A website, system or phone line stops working and the cause is not clear.
- A supplier or customer tells us they were breached.

3. Resolve: the first hour

The incident lead does these in order and writes the time next to each.

1. Write down what you know: who, what, when, which devices and accounts.
2. Disconnect affected devices from the network. Do not delete anything.
3. Change passwords on affected accounts from a device you trust, and turn on two-step sign-in.
4. Call the outside help number on page 1 and tell the insurer if the policy requires it.
5. If money was sent, call the bank immediately and ask for a recall.
6. Decide with the outside help what to restore, and from which backup.

4. Report: who to tell and when

Decide with legal advice whether any law or contract requires a notice, and how soon.

Who	When	Who tells them	Done (time)
Staff	After the first hour	[name]	

Who	When	Who tells them	Done (time)
Customers or partners affected	As soon as facts are confirmed	[name]	
Regulator or authority, if any law applies	[deadline from the law]	[name]	
Insurer	[per policy]	[name]	
Police or national reporting service	If a crime, or funds were lost	[name]	

5. Learn: after the incident

Within two weeks, meet for 30 minutes.

- What happened, in a few sentences.
- What we did well. What we missed.
- Three fixes, each with a name and a date.
- Update this plan and the phone numbers.