Incident Response Plan

Document	Owner	Version	Approved on	Next review
Incident Response Plan	[Name, role]	1.0	[date]	[date, at most 12 months later]

How to use this template
Replace every yellow field. Delete rules that do not apply to your business and add the ones that do. Delete this box and the appendix at the end before you publish or hand the document to a client.
Have the owner approve it and keep the signed copy. This is a template, not legal advice: where a law or a client contract applies, check it.

1. Purpose

This plan tells everyone at [Company name] what to do when something goes wrong with security: a hijacked account, a lost laptop, ransomware, a wrong recipient, data pasted where it should not be. Keep a printed copy: it must work when the network does not.

2. Who does what

Role	Name	Phone (works offline)	Does
Incident lead	[Name]	[...]	Takes charge, decides, keeps the log
Deputy	[Name]	[...]	Takes over if the lead is away
IT / technical	[Name or provider]	[...]	Contains and recovers systems
Communications	[Name]	[...]	Speaks to clients, staff and the press
Legal / data protection contact	[Name]	[...]	Advises on notifying authorities and clients
Management	[Name]	[...]	Approves big decisions and spending

3. How serious is it?

Level	Examples	Response
Low	One phishing email reported and not opened; a lost device that is confirmed encrypted with a strong passcode and no sensitive data cached	Handle the same day; log it; the incident lead confirms the encryption and passcode facts
Medium	A single account taken over with no sign of data access	Incident lead starts this plan within 1 hour; legal assessment if any personal data may be involved

High	Ransomware; several accounts or systems affected; a lost device that is not encrypted or whose encryption is unknown; personal or client data sent to the wrong person, leaked or stolen (suspected or confirmed)	Start this plan at once; management informed; notification decision within 24 hours of first awareness

The label can change as facts come in. **Any suspected breach of personal data goes to the legal or data protection contact straight away, whatever the label.**

4. Steps

1. **Detect and report.** Anyone who suspects an incident calls or messages [security contact]. Write down the time and what you saw.
2. **Take charge.** The incident lead opens the log (section 8) and decides the level.
3. **Contain.** Stop the spread without destroying evidence: disconnect the device from the network (do not switch it off unless told), disable the affected accounts, change passwords and MFA from a clean device, block the sender.
4. **Assess.** What happened, what data and which people or clients are affected, how long, is it still happening? Write facts, not guesses.
5. **Decide on notification.** See section 6. Do not wait for management to confirm before the legal contact is told, and do not stop over a weekend: the legal or data protection contact decides when any legal deadline starts to run. As a company target, aim for a notification decision within 24 hours. If you cannot finish investigating in time, notify with what you know and add the rest later. Write down the decision and the reason, whichever way it goes.
6. **Remove and recover.** Remove the cause (malicious software, rules, access), restore from clean backups, check that systems are clean before reconnecting.
7. **Communicate.** Tell affected people and clients clearly and factually. One person speaks for the company.
8. **Learn.** Within [2] weeks, meet to find what failed and fix it. Update this plan and the training.

5. First hour checklist

☐	Action
☐	Note the time you learned of the incident
☐	Incident lead named and log opened
☐	Affected device(s) disconnected from the network
☐	Affected accounts disabled; passwords and MFA reset from a clean device
☐	Backups checked: are they intact and untouched?
☐	Screenshots or copies of evidence saved (do not alter originals)
☐	Cyber-insurance policy read now: contact the insurer promptly if it requires notice or approval before you hire responders; contact the IT provider under its contract
☐	Notification decision started (section 6)