Incident log and post-incident report

A running incident log to fill in while a site is down or hacked, plus a short post-incident report for the client: timeline, impact, cause, fix and the changes that stop a repeat.

Copy, adapt and send. Replace anything in [brackets] with your own details.

PART 1: INCIDENT LOG (FILL IN AS YOU GO)

- ☐ Incident: [INC-YYYY-MM-DD-01]. Site: [address]. Logged by: [name]. Time zone used: [UTC or local].
- ☐ First noticed: [time], by [monitor / client / customer / you]. Symptom: [exact error or behavior].
- ☐ Confirmed from outside your network: [phone on mobile data / uptime check / curl]. Time: [time].
- ☐ Severity: [down / partly broken / security]. Money affected: [orders, forms, email].
- ☐ Client told: [time, how]. Next update promised by: [time].

TIME WHO ACTION OR FINDING RESULT [00:00] [name] [checked host status page] [no incident listed] [00:05] [name] [read PHP error log] [fatal error in plugin X] [00:12] [name] [renamed plugin folder over SFTP] [site back, admin works] Log every change, even failed ones. Copy exact error text. Save logs and screenshots to [folder].

PART 2: POST-INCIDENT REPORT (SEND WITHIN [2

Subject: [Site name] incident on [date]: summary and next steps

Hi [Client name], here is a short summary of the problem on [date] and what we are doing to stop it happening again.

- ☐ What happened: [one or two plain sentences, no jargon].
- ☐ When: from [start time] to [end time] ([duration]). Detected by: [monitor / report].
- ☐ Impact: [what was affected]. Orders, forms or emails lost: [none known / list].
- ☐ Data and security: [no personal data affected, or what is known and what is still being checked].
- ☐ Cause: [root cause, or "most likely cause" if unproven]. Trigger: [update, attack, expiry].
- ☐ What we did: [the fix, in one or two sentences].
- ☐ What we are changing: [action], owner [name], by [date].
- ☐ Anything we need from you: [approval, access, a decision], by [date].

Reply here if you notice anything still not right. Thanks for your patience, [your name].

BEFORE YOU SEND

- ☐ Keep blame out of it: describe what failed, not who.
- ☐ Do not guess about personal data. If it may be involved, say what you are checking and get advice.
- ☐ Every action has an owner and a date. Add them to the maintenance log and the next monthly check.