

Keep client sites safe, without the drama.

A practical routine for websites and the servers they run on — inspired by the external checks in PCI DSS, without the paperwork.

48h

security releases applied

TLS 1.2+

minimum, older versions off

30 days

encrypted, off-server backups

1 / month

a restore actually tested

This month · October 2026

- 14 Oct** **nginx:** five fixes, in 1.30.6 (stable) and 1.31.7 (mainline).
- 21 Oct** **PHP:** two serious fixes, in 8.2.35, 8.3.36, 8.4.27 and 8.5.12. Branches 8.1 and older get no official fix — they need a vendor backport or an upgrade.
- 21 Oct** **Node.js:** ten fixes, four rated high, in 22.23.4, 24.22.1 and 26.12.1. End-of-life lines get no fix.

THE ROUTINE

Know what you run.

One list of every site: server, web server, PHP or Node.js version, CMS, host, and domain and certificate renewal dates — plus who has access.

Patch on a clock.

Security releases for the OS, web server (nginx, Apache), runtime (PHP, Node.js), CMS core and plugins go on within 48 hours. Name one owner. Restart services after updating.

Retire what's out of support.

Versions past end-of-life get no fixes at all. Plan upgrades before the date, not after.

Watch your dependencies.

Run `composer audit` and `npm audit` in every build. Commit lockfiles. No unpinned installs on live servers. Drop packages you no longer use.

Encrypt properly.

TLS 1.2 or later only. Auto-renewing certificates with expiry alerts. Redirect HTTP to HTTPS, add HSTS, and set the standard security headers.

Control access.

One account per person. Two-factor on hosting panels, DNS, registrar, Git and CMS admin. SSH keys, not passwords. Remove leavers the same day.

Back up, and prove it.

Daily, encrypted, off-server, kept at least 30 days. Restore one site to a staging copy every month. A backup you've never restored is a hope, not a backup.

See problems early.

Monitor uptime, certificate expiry, disk space, errors and file changes. Keep logs at least 90 days. Make sure someone sees an alert out of hours.

Have a plan.

Who gets called, how to put a site into read-only, where the clean backup is, and what you tell the client. Sites that take card payments also need to know who notifies the payment provider.

NEXT STEP

Want a second pair of eyes?

Run our free website health check, or book a consultation. We review, fix and look after websites and servers for agencies and businesses across the UK and Europe.

[Check a website](#)[Book a consultation](#)

chronosweb.hu

Scan to pick a
time that suits
you