Sentrly — WordPress Security Checklist

Hardening basics for any WordPress install — admin, plugins, and headers.

Before launch

- ■ HTTPS works on every URL with no mixed-content warnings.
  Free certificates make this a default; mixed content breaks the trust model.
- ■ HTTP redirects to HTTPS site-wide.
  Otherwise, links and bookmarks bypass your security.
- ■ Strong, unique passwords on every admin account, with 2FA enabled.
  Admin compromise is the single most common cause of small-site breaches.
- ■ Backups are running and tested by restoring once.
  Untested backups are wishful thinking.
- ■ Spam protection on forms (honeypot, captcha, or rate limit).
  Bots will hit forms within hours of going live.

Security headers and configuration

- ■ Strict-Transport-Security set with at least 6-month max-age.
  Locks browsers into HTTPS for your domain.
- ■ Content-Security-Policy at least in report-only mode.
  Catches embedded third-party scripts you didn't intend to allow.
- ■ X-Content-Type-Options: nosniff and Referrer-Policy set.
  Cheap, useful headers with no downside.
- ■ WAF or CDN-level rate limit on /wp-login or /admin equivalents.
  Bots try common admin URLs constantly.

Operations

- ■ Auto-updates on for the platform, plugins, themes, and OS.
  Most exploited vulnerabilities are old and patched.
- ■ Old, unused plugins and themes uninstalled (not just deactivated).
  Inactive code can still be reachable via direct URL.
- ■ File-permission audit: no writable PHP under wp-content unless required.
  Reduces blast radius of an upload bug.
- ■ Monitoring with email/SMS alerts on downtime and unusual login activity.
  Detection beats discovery weeks later.