WP Guard

SECURITY GUIDE

The WordPress PHP Update Checklist



You patched PHP. Before you call it done, walk this list. A missed test is how a fixed hole turns into a broken checkout.

1 Before you patch

- [ ] Note your current PHP version: **Tools > Site Health > Info > Server**.
- [ ] Have a rollback plan, and a staging copy to test on first.
- [ ] Confirm you have a backup you could actually restore from.
- [ ] Check theme, plugin, and custom-code compatibility with the target version.

2 Apply the fix

- [ ] For an emergency fix, patch **within** your branch (e.g. 8.3.30 to 8.3.36), not a branch jump.
- [ ] Confirm the live site is now on the patched release, not just "updated".

3 Test what makes you money

- [ ] Contact and inquiry forms submit, **and** the notification email lands in your inbox.
- [ ] Bookings or appointments go through.
- [ ] Customer accounts: login and password reset.
- [ ] Checkout: cart, payment, and confirmation all complete.
- [ ] File uploads work.
- [ ] Payment and email integrations fire as expected.

4 Test what keeps you running

- [ ] WordPress admin access, on the account you rely on.
- [ ] Your most important pages, loaded on a phone.
- [ ] Integrations: CRM, email platform, anything connected by API.
- [ ] Analytics and tracking are still recording.

5 If something broke

- [ ] Roll back to the previous version, confirm the site is healthy, then isolate the culprit theme or plugin before you try the update again. Do not leave a broken live site while you debug.

RATHER NOT RUN THIS EVERY TIME?

WP Guard watches your WordPress stack for you. On Guaranteed, keeping it patched and tested is **our job, not yours**, and when something breaks, **fixing it is on us**.

wpguard.ai