

20-Point WordPress Security Checklist

Website: _____ Review date: _____

Tick each box after checking it. Record any follow-up work below.

Hosting and PHP

- ☐ Check the current PHP version and security support
- ☐ Review hosting-provider security advisories
- ☐ Confirm HTTPS and SSL certificate validity
- ☐ Check hosting account access and two-factor authentication

WordPress and plugins

- ☐ Check WordPress core updates
- ☐ Review plugin updates and known vulnerabilities
- ☐ Review theme updates
- ☐ Remove unused plugins and themes

Backups and recovery

- ☐ Confirm a recent complete files-and-database backup
- ☐ Check automatic backup schedules
- ☐ Verify off-site backup availability
- ☐ Document or test the restoration procedure safely

Access and protection

- ☐ Review administrator accounts and permissions
- ☐ Enable two-factor authentication where available
- ☐ Check firewall and malware scanning
- ☐ Review security alerts and suspicious logins

Testing and maintenance

- ☐ Test important pages and forms
- ☐ Test checkout and payment functions safely
- ☐ Review scheduled maintenance tasks
- ☐ Record changes and schedule the next review

Follow-up actions

Next review date: _____ Reviewed by: _____

Back up before changes. Test restorations and payments in a safe environment.