Secure Hosting Self-Audit Checklist

20-Point Hosting Security Audit

☐ Is the hosting provider security-focused?
☐ Is server patching current?
☐ Is SSL easy and monitored?
☐ Are backups full and automated?
☐ Are backups stored off-server?
☐ Has restore been tested?
☐ Is DDoS mitigation available?
☐ Is firewall filtering active?
☐ Is malware scanning offered?
☐ Are uptime alerts configured?
☐ Are abuse notices monitored?
☐ Are cPanel/FTP passwords strong?
☐ Is MFA enabled on hosting accounts?
☐ Are dormant access accounts removed?
☐ Is account isolation acceptable?
☐ Is CMS/plugin load supported safely?
☐ Is provider support responsive?
☐ Are incident contacts documented?
☐ Is monthly hosting review scheduled?
☐ Would this host handle compromise calmly?

Scoring:

17–20 = Strong hosting security maturity
12–16 = Moderate infrastructure exposure
0–11 = High foundational weakness