Site builder Guide to WordPress Security - WebTNG.com

Required	Task	Notes
	Site builder task when selecting hosting	
Yes	A reputable hosting service that keeps server software up to date and accounts separate.	
Yes	Select hosting that offers current versions of PHP and MySQL.	
Yes	Select hosting where each site is in its own container, or on shared hosting all sites in account have the same administrator.	
Optional	Select hosting with free Let's Encrypt SSL certificates.	In many cases can save the cost of a separate purchase.
	Site builder task when installing WordPress	
Yes	Change default admin username.	Best done during install. Plugin options available. Can be changed in database.
Yes	Use strong password when installing WordPress.	Built into WordPress, don't override.
Optional	Change the default database table refix.	Best done during install. Plugin options available. Can be changed in database.
	Site builder task when setting up site	
Yes	Use HTTPS and a valid SSL certificate.	Use free Let's Encrypt SSL certificate or purchase other option.
Yes	Check that all links are using HTTPS.	Free 3rd party scanners available for checks.
	Site lockdown tasks	
Yes	Install and configure a WordPress firewall.	Plugin options available
Yes	Use a firewall that gets just-in-time rule updates.	Plugin options available
Yes	Login form brute force protection.	Plugin options available
Yes	Two factor authentication for ecommerce sites, for admins of membership sites, and for other sites with sensitive information.	Plugin options available
Yes	Protect form submissions for all forms on the site.	Plugin options available
Yes	Setup regular backups: daily for most sites, weekly for brochure sites.	Plugin options available
Yes	Store backups offsite	
Yes	Test the backup/restore process.	
Yes	Setup regular malware scans.	Plugin options available
Yes	Setup activity logs.	Plugin options available
Yes	Setup up-time monitoring.	Plugin options available
Yes	Disable XML-RPC if it is not being used.	Plugin options available
Yes	Prevent user enumeration.	Plugin options available
Yes	Check that correct file and directory permissions are in place.	Plugin options available or use hosting control panel
Yes	Disable directory listing	Plugin options available
Optional	Disable the file editor and the ability to install themes and plugins.	Plugin options available
Optional	File change monitoring.	Plugin options available
Optional	Change login URL.	Plugin options available
Optional	Hide that WordPress is being used.	Plugin options available
Optional	Block bot scanners.	Plugin options available
Optional	Disable obscure features.	Plugin options available
	Ongoing maintenance and procedures	
Yes	Keep site up to date including core, themes and plugins.	
Yes	Use strong passwords.	Built into WordPress
Yes	Check that regular malware scans are running.	Plugin options available
Yes	Periodically test the backup/restore process.	
Optional	Periodically change salts.	Plugin options available
Yes	Assign user roles correctly.	

Yes	Manage old user accounts.	Remove unneeded accounts
Yes	Periodically manually check all sites.	Test contact forms, that all updates are inplace, check file system via FTP
Situational Overrides		
Situational	Avoid shared hosting.	Busy sites, ecommerce sites, high profile sites
Situational	Use a network-based firewall solution.	Large ecommerce and high profile sites
Situational	Enforce strong passwords for membership sites.	Plugin options available
Situational	Real time backups of ecommerce transactions for busy ecommerce sites.	High-end hosting provider or plugin-SASS options available
Situational	When managing multiple sites use platform for efficient updating.	Plugin options available
Situational	Third party penetration testing.	For enterprise level sites
Situational	Disaster recovery plan.	For enterprise level sites
Situational	User account audits.	For enterprise level sites