

WEBFORLESS ACADEMY

Website Security Guide

Understand HTTPS, updates, access control, backups, monitoring, secure forms and incident preparation without fear-based marketing.

Practical workbook · Version 2.1.0 · July 2026

How to use this workbook

Work through each section with the people who own the website, content and operations. Record evidence, decisions, owners and review dates. A documented decision is easier to maintain than an assumption.

1. Security is risk management

No website is perfectly secure. The practical objective is to reduce likelihood, limit impact, detect problems quickly and recover reliably. Security decisions should match the value of the data, the complexity of the application and the consequences of downtime or unauthorized access.

Question	Notes / evidence
What is true today?	
What needs to change?	
Who owns the next action?	

2. HTTPS and transport security

HTTPS encrypts traffic between a visitor and the server and helps verify the destination. Certificates should renew automatically, HTTP requests should redirect safely, and mixed-content warnings should be removed. HTTPS does not secure vulnerable code or weak passwords, but it is a basic requirement.

Question	Notes / evidence
What is true today?	
What needs to change?	
Who owns the next action?	

Implementation checklist

■	Security is risk management: Security is strongest when ordinary maintenance is dependable, not when one product promises total protection.
■	HTTPS and transport security: Encryption in transit is one layer, not the whole security program.
■	Updates and dependency control: Every installed component becomes a future maintenance obligation.
■	Authentication and least privilege: The domain account can be as critical as the website server.
■	Backups, monitoring and recovery: A backup is only proven when it can be restored.
■	Secure forms and data handling: Less stored data usually means less risk and less compliance burden.

Review record

Date	Reviewer	Decision or change