Template: Blog Security Checklist Template

Generated: 12/5/2025

Based on Article: "Navigating Security Concerns: Protecting Your Blog and Data"
Website: https://scaleblogger.com

A practical checklist to enhance your blog's security and protect your data effectively.

Checklist Items:

- [ ] **1. Perform a Quick Security Inventory**
  Identify your CMS, active plugins, current themes, and users with administrative access. This helps in prioritizing security fixes.
  Reference Section: Assessing Your Current Security Posture

- [ ] **2. Conduct a Core and Plugin Audit**
  Check your CMS core version and plugin/theme versions for updates. Record the versions and apply updates to ensure they are supported.
  Reference Section: Assessing Your Current Security Posture

- [ ] **3. Validate SSL Configuration**
  Load your site over HTTPS and check for any mixed-content warnings to ensure SSL is properly configured and up to date.
  Reference Section: Assessing Your Current Security Posture

- [ ] **4. Assess User Roles and Privileges**
  Review user roles and ensure that only necessary accounts have administrative privileges. Remove any inactive or unused accounts.
  Reference Section: Securing Access and Authentication

- [ ] **5. Implement Multi-Factor Authentication (MFA)**
  Require MFA for all privileged accounts by enrolling them in an authenticator app and using hardware keys for enhanced security.
  Reference Section: Securing Access and Authentication

- [ ] **6. Setup a Password Policy**
  Enforce the use of a password manager and require passwords to be at least 12 characters long, rotating them only upon compromise.
  Reference Section: Securing Access and Authentication

- [ ] **7. Regularly Audit Security Settings**
  Conduct quarterly reviews of roles, privileges, and account activity to maintain a least-privilege access model.
  Reference Section: Securing Access and Authentication

- [ ] **8. Configure Session Management Settings**
  Establish session timeouts and automated logouts for inactive sessions to prevent unauthorized access.
  Reference Section: Securing Access and Authentication

- [ ] **9. Automate Regular Backups**
  Set up an automated backup schedule to ensure content is preserved and can be restored in case of a breach.
  Reference Section: Protecting Content and Data (Backups & Encryption)

- [ ] **10. Monitor for Anomalous Activity**
  Implement monitoring tools to detect unusual activities or breaches early, allowing for timely incident response.
  Reference Section: Monitoring, Detection, and Incident Response