

WordPress Role Audit Checklist

Complete Guide to Auditing User Roles & Permissions

What is a WordPress Role Audit?

A WordPress role audit is a systematic review of all user accounts, roles, and permissions on your website to identify security risks, remove inactive users, and ensure proper access control.

■ Pre-Audit Preparation

- Schedule audit - Block 2-3 hours of uninterrupted time
- Backup site - Full database and files backup
- Notify stakeholders - Inform team about audit
- Gather tools - User Role Editor, WP Activity Log plugins
- Print this checklist for reference
- Create audit spreadsheet - Track findings and actions

■ User Account Review

- List all users - Export user list with roles
- Count users per role - Administrator, Editor, Author, etc.
- Check last login date - Identify inactive users (90+ days)
- Verify email addresses - Ensure all are valid
- Check for duplicate accounts - Same person, multiple accounts
- Identify test accounts - 'test', 'demo', 'admin2', etc.

■ Administrator Account Audit

- Count Administrator accounts - Should be 1-2 maximum
- Verify each Administrator - Do they still need admin access?

- Check Administrator activity - When did they last log in?
- Demote unnecessary Admins - Change to Editor or lower
- Enable 2FA for all Admins - Two-factor authentication required
- Document Administrator list - Keep record of who has admin access

■ Role Distribution Audit

- Review role distribution - Healthy pyramid structure?
- Check for role inflation - Too many high-level roles?
- Verify role assignments - Does each user have correct role?
- Identify over-privileged users - Users with more access than needed
- Check custom roles - If using custom roles, verify capabilities
- Document role changes - Record any role adjustments made

■ Inactive User Cleanup

- Identify inactive users - No login in 90+ days
- Contact inactive users - Do they still need access?
- Remove confirmed inactive - Delete or downgrade accounts
- Remove former employees - Users who left company
- Remove completed freelancers - Freelancers whose projects ended
- Remove test accounts - Delete all test/demo accounts

■ Security Configuration Audit

- Check password policies - Strong passwords required?
- Verify 2FA status - Enabled for Administrators and Editors?
- Review login limits - Limit login attempts plugin active?
- Check activity logging - WP Activity Log or similar installed?
- Verify user registration settings - Is registration open or closed?
- Review default role - Is default role set to Subscriber?

■ Post-Audit Actions

- Document findings - Create audit report
- Implement changes - Remove users, adjust roles
- Notify affected users - Inform users of role changes
- Update documentation - Update user access documentation
- Schedule next audit - Set reminder for next audit (3-6 months)
- Share report - Share with stakeholders/management

■ Red Flags to Identify During Audit

Critical Red Flags (Fix Immediately)

Red Flag	Risk	Action
5+ Administrator accounts	Critical	Demote to 1-2 immediately
Former employees with access	Critical	Delete immediately
Inactive Administrators (90+ days)	Critical	Demote or delete immediately
Test accounts with Admin access	Critical	Delete immediately
Users with no 2FA (Admins/Editors)	High	Enable 2FA within 7 days

■ *Warning Signs (Fix Within 30 Days)*

Warning Sign	Risk	Action
3-4 Administrator accounts	Medium	Demote to 1-2 within 30 days
Inactive users (90+ days)	Medium	Contact and remove within 30 days
Too many Editors (10+)	Medium	Review and demote unnecessary
Users with outdated emails	Medium	Update or remove within 30 days
No activity logging	Medium	Install WP Activity Log within 30 days

■ Audit Frequency: How Often to Audit

Site Type	Frequency	Why
Ecommerce	Monthly	High security risk, payment data
Membership Sites	Monthly	Member data, payment data
News/Magazine	Quarterly	Many contributors, staff changes
Corporate Sites	Quarterly	Employee turnover, compliance
Agency/Client Sites	Quarterly	Client changes, project completions
Small Business/Blog	Every 6 months	Lower risk, fewer users
Personal Site	Annually	Minimal users, low risk

■ Sample Audit Report Template

WordPress Role Audit Report

Site: _____

Audit Date: _____

Auditor: _____

Next Audit: _____

Executive Summary:

Total users before audit: _____

Total users after audit: _____

Users removed: _____

Roles changed: _____

Administrators before: _____

Administrators after: _____

Findings:

1. _____
2. _____
3. _____

Actions Taken:

■ _____

■ _____

■ _____

Auditor Signature: _____

Date: _____

■ Additional Resources

- WordPress Roles Guide: wprole.com/wordpress-roles-and-permissions/
- Security Best Practices: wprole.com/wordpress-security-best-practices/
- User Role Editor Plugin: wordpress.org/plugins/user-role-editor/