



## SOP for Security and Maintenance in WordPress

### Procedure:

#### Regular Updates (WordPress, Themes, Plugins)

- Step 1: Log in to the WordPress admin dashboard regularly to check for available updates for WordPress core, themes, and plugins.
  - Tools/Resources Needed: WordPress admin access.
  - Tips: Schedule regular weekly or bi-weekly checks to ensure timely updates.
- Step 2: Before updating, ensure that backups are current to prevent data loss in case of update conflicts or errors.
- Step 3: Update WordPress core when notifications appear in your dashboard. Proceed with theme and plugin updates by navigating to "Dashboard" > "Updates" and following the prompts to update each item.
  - Tips: Perform updates during low-traffic periods and test on a staging site if possible to minimize impact on live site functionality.

#### Backups (Manual and Automated Solutions)

- Step 1: Choose a backup solution that fits your needs, which could be a plugin (e.g., UpdraftPlus, BackupBuddy) or your hosting provider's backup service.
- Step 2: Set up regular automated backups through your chosen solution. Opt for at least daily backups for active sites and ensure that both your site's files and database are included.
  - Step 3: Store backups in a secure, off-site location. Many backup solutions offer integrated cloud storage options (e.g., Google Drive, Dropbox).
    - Tips: Periodically test your backups by restoring from backup to a staging environment to ensure they are functioning correctly.

#### Security Checks and Improvements

- Step 1: Implement a security plugin (e.g., Wordfence, Sucuri) to enhance your site's security with features like firewall protection, malware scanning, and security hardening.

- Step 2: Conduct regular security scans using your security plugin to check for malware, vulnerabilities, and unauthorized access attempts. Review scan results and take necessary actions to address any issues.
  - Step 3: Strengthen login security by implementing measures such as two-factor authentication, strong passwords, and limiting login attempts to prevent brute force attacks.
- Step 4: Keep abreast of WordPress security best practices and updates. Regularly review and update your site's security measures.
  - Tips: Consider subscribing to WordPress security blogs or newsletters for the latest security tips and vulnerability alerts.

Safety/Compliance Considerations: Ensure compliance with relevant data protection regulations (e.g., GDPR) by securing user data and providing transparent data handling policies. Regularly review your site's compliance and adjust security practices as needed.