WordPress Website Hardening Guidelines

1.0– Updates to WordPress Themes and Plug-ins

#	Hardening Procedures	Status
1.1	Ensure that WordPress is updated to the latest version.	
1.2	Consider configuring automatic WordPress updates.	
1.3	Ensure that all WordPress themes and plug-ins are updated to the latest version.	
1.4	Consider configuring automatic WordPress theme and plug-in updates.	
1.5	Delete all unused themes or plugins.	
1.6	Remove WordPress Version from head META DATA	

2.0– Accounts and Passwords

#	Hardening Procedures	Status
2.1	All passwords should be updated to meet minimum password strength requirements.	
2.2	Consider a WordPress plug-in to enforce strong password requirements.	
2.3	Create a new administrator account with a unique username and strong password.	
2.4	Delete any default administrator or user accounts.	
2.5	Consider enabling two-step authentication. (if possible)	
2.6	Limit the number of login attempts to 3 attempts.	
2.7	Require a CAPTCHA for all login pages.	
2.8	Utilize automatic password generators and storage tools	

Plug-ins to consider:

1. Enforce strong password requirements. (Wordfense)
2. Enforce limited login attempts. (Lock Down, Secured Logins)
3. Hide Back End Login. (Hide Login)
4. Lock Down WP-Admin (WP Admin)

3.0- File Permissions and Securing Key Folders

#	Hardening Procedures	Status
3.1	The following folders/files should be configured to be writable to only the administrator account: - /wp-admin/ - /wp-includes/ - /wp-content/ - /wp-content/themes/ - /wp-content/plugins/	
3.2	Add server-side password protection to the wp/admin/ page.	
3.3	Disable file editing within WordPress	
3.4	Secure wp-includes # Secure wp-config.php <files wp-config.php> order allow,deny deny from all </files>	
3.5	Secure Wp-config.php	
3.6	Move wp-config.php [You can move the wp-config.php file to the directory above your WordPress install. This means for a site installed in the root of your web space, you can store wp-config.php outside the web-root folder and it will not be available to the web.]	
3.7	Consider the installation of a Web Firewall (WAF) to the web server. (Calm AV)	

Plug-ins to consider:

1. Security Plug-ins (All in One WP Security)

4.0– Data Backups, Logging, and Monitoring

#	Hardening Procedures	Status
4.1	Automatically backup the MySQL database on a periodic basis.	
4.2	Change Database prefix for WordPress Installations	
4.3	Encrypt all data backups and/or backup to read only media.	
4.4	Install forensic logging devices or plugins.	
4.5	Install an intrusion detection device or plugins.	

Plug-ins to consider:

1. Backup & Restore (Updraft,)
2. Backup Scheduler (Scheduler)
3. WP Backup (WP Backup)

5.0 – Manual Control Considerations

#	Hardening Procedures	Status
5.1	Gather key login detail from Website developer and ensure ownership is completely transferred including: - Server login - WordPress login - URL ownership and hosting - all files and images	
5.2	Ensure individuals are assigned to perform the following functions: - receive and respond to backup alerts and failures - receive and respond to intrusion detection alerts - receive and respond to password failures - receive and respond to alerts for updates, theme updates, and plug-in updates	
5.3	Develop a documented incident response plan in the event of website security breach of defacement. Events include: - backup alerts and failures - intrusion detection alerts - password failures - alerts for updates, theme updates, and plug-in updates	
5.4	Develop a documented backup and disaster recovery plan in the event of website outage.	