**Friends of Smithgall Woods**

**Security Plan Implementation**

**11/2/2017**

1. Changed 1and1.com account password.
2. Changed FTP passwords.
3. Changed WordPress passwords.
4. Deleted suspicious files from October 29, 2017, attack.
5. Deleted the following WordPress plugins: SEO Meta Tags, Mail Chimp, Hello Dolly, and Akismet
6. Updated “Pages Link To” WordPress plugin. The Volunteer Hours login depends on this plugin.
7. Updated “NextGEN Gallery” WordPress plugin. The Photo Gallery page depends on this plugin.
8. Deleted WordPress theme “2010.”
9. Removed original “base64” encoded bad code in wp-includes\locale.php file. It was previously commented out to prevent it from executing.
10. Per <http://www.wpbeginner.com/wp-tutorials/how-to-disable-php-execution-in-certain-wordpress-directories/>, I created an .htaccess file to disable PHP execution in the following directories: /wp-includes and /wp-content/uploads. However, placing the file in the /wp-includes folder made the text white in the WP admin console where you edit the pages, so it was removed from that folder.
11. Backed up the website. Currently have two backups of the website: One from 9/5/17 and one from 11/1/17.
12. Updated PHP. Updated to 5.6 first and did not encounter any problems. After updating WordPress to the newest version, we tried updating PHP to 7.0, since that’s what both WP and the hosting site recommend. However, it broke the login page to the volunteer hours app, so we rolled it back to version 5.6.
13. Updated WordPress to newest version. It only took a few seconds, and there were no issues with the site afterward.
14. Deleted all FTP accounts except the main one: u48922589. The rest provided no additional access and so were deemed unnecessary.
15. Deleted the “admin” WordPress account. Accounts that use a default name like “admin” are hacking targets, and the account appeared to be unused, so it was deemed unnecessary.