**Friends of Smithgall Woods**

**Website Security Remediation Plan**

1. Remove all unnecessary accounts, then change the remaining account passwords. The following accounts are active:
   1. Hosting site
      1. 17505820 – Dr. Huber’s account
   2. Databases
      1. [db357026991](https://my.1and1.com/mysql-database-details/db357026991?__lf=ftp_create_account_flow) (FSGW) – Still investigating.
      2. [db358933030](https://my.1and1.com/mysql-database-details/db358933030?__lf=ftp_create_account_flow) (FSGWData) – Still investigating.
      3. [db360322876](https://my.1and1.com/mysql-database-details/db360322876?__lf=ftp_create_account_flow) (Fresh root WP install) – This is the database the WordPress site pulls from and saves to for page content.
      4. [db265662256](https://my.1and1.com/mysql-database-details/db265662256?__lf=ftp_create_account_flow) (login and hours database) – This is the volunteer hours database.
      5. [db268336715](https://my.1and1.com/mysql-database-details/db268336715?__lf=ftp_create_account_flow) (calendardb) – Still investigating.
   3. FTP accounts
      1. [u48922589](https://my.1and1.com/ftp-account-details/54939311?__lf=ftp_create_account_flow)
      2. [u48922589-drdan](https://my.1and1.com/ftp-account-details/75464305?__lf=ftp_create_account_flow) – This is the only account we can access. The passwords for the others are incorrect. Since only one account is necessary, we recommend deleting all but one account.
      3. [u48922589-students](https://my.1and1.com/ftp-account-details/76946453?__lf=ftp_create_account_flow)
      4. [u48922589-Admin](https://my.1and1.com/ftp-account-details/77483152?__lf=ftp_create_account_flow)
   4. WordPress accounts
      1. mhuber ([mhuber@uga.edu](mailto:mhuber@uga.edu))
      2. admin ([youdomaincom977@gmail.com](mailto:youdomaincom977@gmail.com)) – This is the default admin account in WordPress. We don’t know whose email address that is.
      3. Admin1 ([webmaster@friendsofsmithgallwoods.org](mailto:webmaster@friendsofsmithgallwoods.org)) – Who is responsible for the Webmaster email account?
      4. lcompton ([compton.pl@gmail.com](mailto:compton.pl@gmail.com)) – Who is Larry Compton?
2. Update all website software.
   1. WordPress – Running version 4.5.9, update to 4.8.1
   2. PHP – Running version 5.2, update to 7.0
   3. WordPress theme – There is no update for this theme; it’s six years old.
   4. WordPress plugins
      1. Akismet – Running version 3.0, update to 3.3.4
      2. NextGEN Gallery – Running version 1.7.4, update to 2.2.12
      3. Page Links To – Running version 2.4, update to 2.9.9
      4. Seo Meta Tags – Running version 1.0, update to 1.4
3. Use the hosting website’s security application to help prevent further issues.
   1. 1&1 SiteLock - <https://help.1and1.com/hosting-c37630/sitelock-c85170/what-is-1and1-sitelock-a792625.html>
      1. Basic ($.99/month)
         1. Daily malware scan
         2. Trust Seal
         3. Search engine blacklist monitoring
         4. SSL verification
         5. Web app scan (on demand once a month)
         6. SQL injection scan (on demand once a month)
         7. XSS scan (on demand once a month)
         8. Number of pages monitored – 25
      2. Premium ($4.99/month)
         1. Daily malware scan
         2. Trust Seal
         3. Search engine blacklist monitoring
         4. SSL verification
         5. Web app scan
         6. SQL injection scan
         7. XSS scan
         8. File Change Monitoring
         9. Number of pages monitored – 500

Note that for the updates the website would need to be down for a short period of time. This could be accomplished during a late evening/early morning timeframe of the client’s choice.