NeoSOFT™ TECHNOLOGIES

CMMI LEVEL 3

Wordpress Guidelines

Project Name: _____

Client: _____

Date:_____

Section 1: Installation and upgrade

1. Download the wordpress from http://wordpress.org/download/ and install the latest version of WP.
2. While installation just make sure username should **not** be “admin” and password should be a **random** string.
3. If possible try to set the prefix as projectname_ instead of wp_.
4. Please use ftp while installation of plugins and never save FTP details on the WP admin.
5. Take backup of code and SQL before upgrade of any plugin or WP.

Section 2: Security

1. Secure admin section by adding below code.

   Create **.**htaccess file with following content in it.

   order deny,allow

   allow from 202.090.21.1 (replace with your IP address)

   deny from all

2. Secure Wordpress

   Create .htaccess file with following content in root.

   ```
   # BEGIN WordPress
   <IfModule mod_rewrite.c>
   RewriteEngine On
   RewriteBase /
   RewriteRule ^index\.php$ - [L]
   RewriteCond %{REQUEST_FILENAME} !-f
   RewriteCond %{REQUEST_FILENAME} !-d
   RewriteRule . /index.php [L]
   </IfModule>
   ```

```
# END WordPress

<Files wp-login.php>
Order Deny,Allow
Deny from all
Allow from 206.183.111.25 (replace with your IP address)
</Files>

<Files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</Files>

<files wp-config.php>
Order deny,allow
Deny from all
Allow from 206.183.111.25 (replace with your IP address)
</files>

# protect from injection
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} proc/self/environ [OR]
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
RewriteCond %{QUERY_STRING} base64_encode.*(.*) [OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

3. Install Wordpress Wordfence plugin, ask customer to buy the subscription for the plugin from http://www.wordfence.com/. If client is not willing to buy then use free key. Periodically scan the wordpress for vulnerability and update the plugin(Make sure you have backup the code and sql before upgrade).

Section 3: Development

1. Try to avoid using of plugins, all unused plugins should be uninstalled and deleted before making it live.
2. Use http://wordpress.org/extend/plugins/wp-migrate-db/ for migration.
3. If anyone using wordpress http://wordpress.org/extend/plugins/advanced-custom-fields/ plugin and if website is heavy content driven just make sure wp_options table is optimized, specifically field autoload = 'yes' will overload the memory by loading all rows in memory. This can manage by adding hooks like

   add_option('option_name', 'option_value', '', 'no'); // 'no' = not autoload

   or write a cron which will update the autoload values to no.