# Security Plan

eLearnReady LLC

## A. SSL Certificates

SSL certificates keep our site and online transactions secure with strong encryption, protecting any sensitive data our site is collecting. We employ SSL Certificates from GlobalSign, one of the most respected names in the industry.

## B. Server Security

Our server employs the following methods to tighten the security of our server/sites:

- ✓ **Firewall Protection**
  Traffic is processed by the firewall before it reaches our server. This means that threats are eliminated before they reach our server and the processing will not affect the performance of our primary server. Our adaptive network security solutions provide signature based intrusion prevention that automatically blocks malware, such as Trojan horses, worms, and spyware.

- ✓ **Block specific IP addresses and user agents from accessing the site**
  We completely ban hosts and user agents from our site without having to manage any configuration. Any IP addresses or user agents found in our blacklists will not be allowed any access to our site.

- ✓ **Force SSL for any post, page, or admin page**
  We redirect all http page requests to https to secure all online transaction.

- ✓ **HTTP Intrusion Protection**
  Intrusion detection (ID) is used to monitoring and analyzing both user and system activities on our server.

- ✓ **Local brute and XML-RPC force protection**
  We protect our site against attackers that try to randomly guess login details to our site.

- ✓ **Network brute force protection**
  Network brute force protection bans users who have tried to break into other sites from breaking into ours. The network protection will automatically report the IP addresses of

failed login attempts to iThemes network and will block them for a length of time necessary to protect our site based on the number of other sites that have seen a similar attack.

- ✓ **Scheduled malware scanning powered by Sucuri SiteCheck**
  This method protects our site with automated malware scans. Our site is automatically scanned each day. If a problem is found, an E-mail is sent to our network administrator.

- ✓ **Remove login error messages**
  By default, WordPress shows error messages when someone enters an incorrect username or password on the login page. These error messages can be used to guess a username, user email address, or password. In our site, we've disabled login hints and login error messages.

- ✓ **Monthly Nessus Vulnerability Scans**
  Tenable's Nessus vulnerability scans are used in scanning for potential compromises to our hosting environment.

- ✓ **Remove RSD header info**
  By removing RSD (Really Simple Discovery) header, our site blocks common forms of attacks.

- ✓ **Remove Windows Live Write header information**
  Our site doesn't use Window Live Writer or other blogging clients that rely on this file. As such, it is removed for better protection.

- ✓ **SSH / cPanel / FTP Hardening**
  SSH / cPanel / FTP securities are tightened by modifying the corresponding configure files.

- ✓ **Web Server & PHP Hardening**
  Web server and PHP securities are hardened by preventing public access to system files, disabling directory browsing, filtering request methods, filtering suspicious query strings in the URL, filtering non-English characters, filtering long URL strings, and removing file writing permissions.

- ✓ **File Change Detection**
  If someone manages to get into our site, they'll probably add, remove or change a file. We receive E-mail alerts showing any recent file changes.

- ✓ **404 Detection**
  If a bot is scanning our site for vulnerabilities, it will generate a lot of 404 errors. Our security system will lock out that IP after the limit (10 errors in 30 minutes). The IP will be released after 30 minutes.

- ✓ **Lock Out Bad Users**
  Keep bad users away from our site if they have too many failed login attempts, if they generate too many 404 errors, or if they're on a bot blacklist.

- ✓ **Hide Login & Admin**
  We have changed the default URL of our WordPress login area so attackers won't know where to look.

- ✓ **Email Notifications**
  On daily basis, we receive E-mail notifications when someone gets locked out after too many failed login attempts or when a file on our site has been changed.

- ✓ **Change WordPress Salts & Keys**
  Our server makes updating our WordPress salts & keys on monthly basis. Updating these authentication keys every so often adds another layer of complexity.

- ✓ **Online File Comparisons**
  Our server compares changes made to any WordPress core file on our system with the version on WordPress.org to determine if the change was malicious.

## C. Database Backups

Two backups are performed on daily basis. First, the database is backed up and sent to a secure Email account. Second, database and entire site files are fully backed up and sent to offsite storage destinations with encryption protection. In the event of a system failure, the website can be restored.