IPP Security Review Questionnaire

Today's Date: *July 14, 2016*

Company Information

Company Name: *Strat Pad Inc*

Street Address: *185 - 911 Yates St.*	Office Phone: *(415) 655-1082*	Office Fax: *( )*

P.O. Box:	City: *Victoria*	State: *BC*	ZIP Code: *V8V 4Y9*

Total Number of Customers You Expect to Use Your Application: *100,000 +*

Number of Existing Customers: *100,000*

Contact Information

Contact Name: *Julian Wood*	Contact Email Address: *julian@stratpad.com*	Contact Phone: *(403) 585-7227*

Employer: *Strat Pad Inc.*	Employer Address: *185-911 Yates St.*	Employer Phone: *(415) 655-1082*

Application Information

Application ID: *b7pm 8tj f3i*

IPP API Calls Used (example: getAccount):
companyInfo   preferences
reports

APPLICATION SECURITY DETAILS

WEB APPLICATION SCANNING

Cross Site Scripting Vulnerabilities	You certify that your application has been tested for Cross Site Scripting Vulnerabilities, and any issues found have been resolved. This includes reflected and stored cross site scripting vulnerabilities.	☒
XML Injection Vulnerabilities	You certify that your application has been tested for XML Injection Vulnerabilities, and any issues found have been resolved.	☒
SQL injection vulnerabilities	You certify that your application has been tested for SQL Injection Vulnerabilities, and any issues found have been resolved.	☒
Cross Site Request Forgery Vulnerabilities	You certify that your application has been tested for Cross Site Request Forgery Vulnerabilities, and any issues found have been resolved.	☒

APPLICATION CODE		
Session/Tokens	You certify that no Intuit Token is exposed in a query string, log, or error message within your application.	☒
Cookies	You certify that all application session cookies have the following attributes set: 1. Secure 2. HTTPOnly	☒
Disable Caching for SSL Pages	You certify that caching has been disabled on all SSL pages and all pages that contain sensitive data by using value "no-cache" instead of "private" in "Cache-Control" header.	☒
AUTHENTICATION KEYS		
Authentication Key Storage	*Your application must encrypt the Private Key Password, Consumer Key and Secret.* Encrypt the Private Key Password, Consumer Key, and Secret with a symmetric algorithm (3DES, AES). AES is preferred. Store your AES key in your application, in a separate configuration file. Decrypt the keys and store them in the user session for use (and transient, so that they do not get persisted if the session is suspended/terminated).	☒
APP SERVER CONFIGURATION SETTINGS		
SSL Settings	SSL must be configured to support only SSL version 3 or TLS version 1 with a minimum key size of 128.	☒
Insecure HTTP Methods Disabled	The application web server must be configured to disable the TRACE and other HTTP methods if not being used.	☒
HTTPS Settings	HTTPS is enforced on all pages of your application.	☒
Server Baseline	You certify that your OS, Web Server, and/or App Server are initially setup in a security-hardened configuration.	☒
Server Patching	You certify that all OS, Web Server, and/or App Server security patches are up to date at this time, and that new patches are applied in a commercially reasonable timeframe after they are made available by the hardware and software vendors.	☒
INTUIT PARTNER PLATFORM DATA		
Data Use	I certify that I will not export, save, or store IPP data for any other purposes than the functional use of my application.	☒
Data Access	I certify that no external APIs in my application will allow access to my customer's IPP data.	☒

Signature

My signature below indicates the above information is true to the best of my knowledge, and my application conforms to all the items in the above checklist. I understand that Intuit, or a third-party Intuit security partner, may validate the security of my application at any time to ensure ongoing compliance with the security requirements listed in the checklist. I also understand that Intuit may revoke my production access if the application is not compliant with the security requirements included in this checklist. And that the security requirements are subject to change by Intuit at any time, and I am responsible for ensuring compliance within a commercially reasonable timeframe after being notified by Intuit.

Julian Wood

Name

CTO

Title

Signature *Julian Wood*

Date July 14, 2016