VP-ASP Shopping Cart

PCI Compliance Questionnaire Responses

17th October 2008

Private and Confidential

1. Introduction

VP-ASP & Payment Card Industry Data Security Standard (PCI-DSS):

This document has been created to assist you with how to answer the questions in the Self Assessment Questionnaire.

Our suggested answers are based on using VPASP Version 7.xx or higher.

Not all questions are to do with the VP-ASP Shopping Cart. Many of the questions have to do with your environment and must be answered according to the relevant set up your business has in place.

Some of the questions may for example have to do with where your web site is hosted or how you take offline credit card payments.

This document assumes you are using the default VPASP package straight out of the box with no modifications and are using a PCI Compliant gateway provider from our list of supported PCI Compliant partners.

If any customisation is made to the code to allow the storage of sensitive card data the advice in this document is invalidated and a full security audit by a qualified certified auditing company will need to be performed on your entire environment.

2. PA-DSS Security Audit Procedures

The following questions have been listed so the main question and the answer are easily readable. These answers are only a guide and you should when filling in the self assessment ensure that each question is answered correctly for your environment.

PA-DSS Requirements	VPASP Status
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system.
2. Protect stored cardholder data	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system.
3. Provide secure authentication features	Access to the VPASP online administration tool is gained using encrypted username and password details. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
4. Log payment application activity	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
5. Develop secure payment applications	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
6. Protect wireless transmissions	Not applicable to VPASP. Even though not applicable to VPASP your business may still take payments using wireless technology so it is up to you to verify this section of your business practices.
7. Test payment applications to address vulnerabilities	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
8. Facilitate secure network implementation	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system.

	As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
9. Cardholder data must never be stored on a server connected to the Internet	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
10. Facilitate secure remote software updates	Not applicable to VPASP.
11. Facilitate secure remote access to payment application	VPASP does not store or retain any card holder data. All secure data is handled by the payment gateway with no data being entered into the VPASP system. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
12. Encrypt sensitive traffic over public networks	All customer data entry points within VPASP will redirect to use SSL automatically. The merchant must obtain a dedicated SSL certificate for this system to operate successfully.
13. Encrypt all non-console administrative access	Access to the VPASP online administration tool is gained using encrypted username and password details. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
14. Maintain instructional documentation and training programs for customers, resellers, and integrators	VPASP Payment gateway interfaces are provided with instructions on implementation to ensure PCI Compliance requirements are followed.