2019

VP-CART PCI Compliance Questionnaire Responses

PRIVATE AND CONFIDENTIAL

Rocksalt International Pty Ltd.

CONFIDENTIALITY

The information contained within this proposal is confidential and the contents of this document may not be disclosed in whole or in part to any other party without the prior written consent of RockSalt PTY Ltd.

1. Introduction

VP-CART & 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 VPCART9.xxxorotherhigherversions.

Not all questions are related with the VP-CART Shopping Software. 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.

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

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	VP-CART Status
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data	VPCART 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 VPCART system.
2. Protect stored cardholder data	VPCART 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 VPCART system.
3. Provide secure authentication features	Access to the VPCART 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	VPCART 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 VPCART 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	VPCART 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 VPCART 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 VPCART. Even though not applicable to VPCART 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	VPCART 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 VPCART 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	VPCART 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 VPCART system. As the card data is stored at the payment gateway you will need to ensure that your payment gateway supports this requirement.
9. Card holder's data must never be stored on a server connected to the internet	VPCART 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 VPCART 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 secured remote software upgrade	Not applicable to VPCART
11. Facilitate secured remote access to payment application	VPCART 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 VPCART 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 network	All Customer entry data point with VPCART 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 VPCART administrative online tool is gained through using User 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	VPCART Payment gateway interfaces are provided with instructions on implementation to ensure PCI Compliance requirements are followed.