HelpVet.Net

Payment Card Security Policies

For PCI DSS version 3.2

Version 1.1 - May 22, 2019

Revision History

Changes	Approving Manager	Date
Initial Publication	Steve Wilson	5-22-2019

Introduction and Scope

Introduction

This document explains HelpVet.net's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. HelpVet.net management is committed to these security policies to protect information utilized by HelpVet.net in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, HelpVet.net does not store cardholder data in electronic format, nor does it process or transmit any cardholder data on their systems or premises. Retention of cardholder data, if any, shall be limited to paper reports or receipts.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) A, version 3.2 revision 1.1, released January 2017. Should HelpVet.net implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ A, it will be the responsibility of HelpVet.net to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

HelpVet.net shall verify that all vendor-supplied defaults are changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1.a)

All unnecessary default accounts must be removed or disabled before installing a system on the network. (PCI Requirement 2.1.b)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Implement Strong Access Control Measures

These requirements are applicable for all accounts with administrative capabilities and all accounts used to view or access cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by cardholders and are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

Assign all users a unique ID before allowing them to access system components or cardholder data. (PCI Requirement 8.1.1)

Immediately revoke access for any terminated users. (PCI Requirement 8.1.3)

Verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment. (PCI Requirement 8.2)

Passwords must have a minimum length of at least seven characters and contain both numeric and alphabetic characters. (PCI Requirement 8.2.3)

Disable or remove any group, shared, or generic IDs and passwords. (PCI Requirement 8.5)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI Requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)

Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)

Any transfer of media must be explicitly approved by an appropriate member of management. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI Requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Any container storing information prior to destruction must be secured (locked) to prevent unauthorized access to the contents. (PCI Requirement 9.8.1)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Service Providers

HelpVet.net shall implement and maintain policies and procedures to manage service providers. (PCI Requirement 12.8)

This process must include the following:

Maintain a list of service providers (PCI Requirement 12.8.1)

Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI Requirement 12.8.2)

Implement a process to perform proper due diligence prior to engaging a service provider (PCI Requirement 12.8.3)

Monitor service providers' PCI DSS compliance status (PCI Requirement 12.8.4)

Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI Requirement 12.8.5)

HelpVet.net shall create an incident response plan to be implemented in the event of system breach. (PCI Requirement 12.10.1)