



# Sage Payment Solutions

## PA-DSS Implementation Guide

Version 1.0 - 02/25/2010

### **CONFIDENTIAL INFORMATION**

This document is the property of Sage Payment Solutions; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by

anyone other than the intended recipient is strictly prohibited without prior written permission of Sage Payment Solutions.

# Revision History

Changes	Approving Manager	Date
Initial Publication		

# Table of Contents

<b>1</b>	<b>INTRODUCTION AND SCOPE.....</b>	<b>5</b>
1.1	Introduction.....	5
1.2	What is Payment Application Data Security Standard (PA-DSS)?.....	5
1.3	Distribution and Updates .....	5
1.4	Versions .....	5
<b>2</b>	<b>SECURE DELETION OF SENSITIVE DATA AND PROTECTION OF STORED CARDHOLDER DATA.....</b>	<b>6</b>
2.1	Merchant and Reseller/Integrator Applicability .....	<b>Error! Bookmark not defined.</b>
2.2	Secure Deletion Instructions .....	<b>Error! Bookmark not defined.</b>
<b>3</b>	<b>PASSWORD AND ACCOUNT SETTINGS .....</b>	<b>8</b>
3.1	Access Control.....	8
3.2	Passwords .....	<b>Error! Bookmark not defined.</b>
<b>4</b>	<b>LOGGING.....</b>	<b>9</b>
4.1	Merchant Applicability .....	9
4.2	PCI Guidelines for Logging .....	<b>Error! Bookmark not defined.</b>
4.3	Configuring Log Settings.....	<b>Error! Bookmark not defined.</b>
<b>5</b>	<b>WIRELESS NETWORKS .....</b>	<b>10</b>
5.1	Merchant Applicability .....	10
5.2	PCI Requirements .....	10
<b>6</b>	<b>NETWORK SEGMENTATION .....</b>	<b>11</b>
6.1	Merchant Applicability .....	11
<b>7</b>	<b>SECURE REMOTE SOFTWARE UPDATES.....</b>	<b>12</b>
7.1	Merchant Applicability .....	12
7.2	Acceptable Use Policy .....	<b>Error! Bookmark not defined.</b>
7.3	Personal Firewall.....	12
7.4	Remote Update Procedures .....	12
<b>8</b>	<b>REMOTE ACCESS.....</b>	<b>13</b>
8.1	Merchant Applicability .....	13
8.2	Remote Access Software Security Configuration .....	13
<b>9</b>	<b>ENCRYPTING NETWORK TRAFFIC.....</b>	<b>15</b>
9.1	Transmission of Cardholder data.....	15
9.2	Email and Cardholder data.....	15
9.3	Non-Console administrative access .....	15

# 1 INTRODUCTION AND SCOPE

## 1.1 Introduction

The purpose of this PA-DSS Implementation Guide is to instruct merchants, resellers and integrators on how to implement Solutions' Sage Exchange Version 1.0 into their environment in a PA-DSS compliant manner. It is not intended to be a complete installation guide. Sage Exchange, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI compliance.

## 1.2 What is Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) is a set of security standards that were created by the PCI SSC to guide payment application vendors to implement secure payment applications.

## 1.3 Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants, resellers and integrators. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as changes in the PA-DSS standard.

Updates to the PA-DSS Implementation Guide can be obtained by <INSERT METHOD OF OBTAINING UPDATES>.

## 1.4 Versions

This PA-DSS Implementation Guide references both the PA-DSS and PCI requirements. The following versions were referenced in this guide.

- PA-DSS version 1.2
- PCI DSS version 1.2

## 2 SECURE DELETION OF SENSITIVE DATA AND PROTECTION OF STORED CARDHOLDER DATA

**PA-DSS 1.1.4** Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the software.

Include the following instructions:

- That historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software).
- How to remove historical data.
- That such removal is absolutely necessary for PCI compliance.

Sage Exchange v1 is the first version of the software. Sage Exchange does not store any sensitive authentication data (including magnetic stripe data and card validation values or codes).

**PA-DSS 1.1.5** Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems.

Include the following instructions:

- That sensitive data (pre-authorization) must only be collected when needed to solve a specific problem.
- That such data must be stored only in specific, known locations with limited access.
- That only a limited amount of such data must be collected as needed to solve a specific problem.
- That sensitive authentication data must be encrypted while stored.
- That such data must be securely deleted immediately after use.

Sage Exchange does not store any sensitive authentication data (including magnetic stripe data and card validation values or codes). Sage Exchange v1 payment application does not have the functionality to collect sensitive authentication data for troubleshooting.

**PA-DSS 2.1** Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.

Include the following instructions:

- That cardholder data must be purged after it exceeds the customer-defined retention period.
- That cardholder data must be purged at all locations where the payment application stores cardholder data.

Cardholder data must be purged after it exceeds the customer-defined retention period.

Sage Exchange v1 software does not store any cardholder data.

**PA-DSS 2.7** Securely delete any cryptographic key material or cryptogram stored by previous versions of the software. This could be cryptographic keys used for computation or verification of cardholder data or sensitive authentication data.

Include the following instructions:

- That cryptographic material must be removed.
- How to remove cryptographic material.
- That such removal is absolutely necessary for PCI compliance.
- How to re-encrypt historic data with new keys.

Sage Exchange v1 is the first version of the software. Sage Exchange v1 software does not store any cardholder data. There is no cryptographic key material stored by Sage Exchange.

## Disable Windows Restore Points

On Windows XP systems "System Restore Points" must be disabled. To do this follow the below instructions:

1. Click Start.
2. Right-click My Computer, and then click Properties.
3. On the System Restore tab, check Turn off System Restore or Turn off System Restore on all drives.

NOTE: If you do not see the System Restore tab, you are not logged on to Windows as an Administrator.

4. Click Apply.
5. When you see the confirmation message, click Yes.
6. Click OK.

More information can be found on Microsoft's Support Website:

<http://support.microsoft.com/kb/310405>

## 3 PASSWORD AND ACCOUNT SETTINGS

### 3.1 Access Control

Merchants, resellers and integrators are advised to control access, via unique username and PCI DSS compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Sage Exchange v1 payment application does not have any administrative users or store any cardholder data.

However, **merchants must control access, via unique username and PCI DSS compliant complex passwords, to any PCs, Servers with Sage Exchange payment application.**

The following guidelines should be followed to protect the operating system:

Passwords should meet the requirements set in PCI DSS section 8.5.8 through 8.5.15, as listed here.

**PCI DSS 8.5.8** – Do not use group, shared, or generic accounts and passwords.

- Ensure that shared and generic user IDs are not used to administer any system components.
- Ensure policies/procedures explicitly prohibit group and shared passwords.
- Ensure that group and shared passwords are not distributed, even if requested.

**PCI DSS 8.5.9** – Passwords must be changed at least every 90 days.

**PCI DSS 8.5.10** – Passwords must be at least seven characters in length.

**PCI DSS 8.5.11** – Passwords must be including both alphabetic and numeric characters.

**PCI DSS 8.5.12** – New passwords cannot be the same as any of the last four passwords used.

**PCI DSS 8.5.13** – If an incorrect password is provided six times the account should be locked out.

**PCI DSS 8.5.14** – Account lockout duration should be at least 30 minutes (or until an administrator resets it).

**PCI DSS 8.5.15** – Sessions idle for more than 15 minutes should require re-entry of username and password to re-activate the session.

#### **PA-DSS Requirements Reference:**

**3.1** Application as provided by vendor must require unique usernames and secure authentication for all administrative access and for all access to cardholder data.

**3.2** Access to PCs, servers, and databases with payment applications must require a unique username and secure authentication.

## 4 LOGGING

### 4.1 Merchant Applicability

Currently, for Sage Exchange version 1, there is no end-user, configurable, logging settings.

Sage Exchange v1 payment application does not use any administrative accounts. It also does not provide administrative access to any functions that change settings that may affect PADSS compliance. No cardholder data is stored by the application. Since log settings are built around access to cardholder data and administrative functions that affect PADSS compliance, audit logging does not apply to the Sage Exchange v1 payment application.

## 5 WIRELESS NETWORKS

### 5.1 Merchant Applicability

If wireless is used or implemented in the payment environment or application, the wireless environment must be configured per PCI DSS version 1.2 requirements 1.2.3, 2.1.1, and 4.1.1. Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure.

### 5.2 PCI Requirements

**PCI DSS 1.2.3** - Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

**PCI DSS 2.1.1** – Ensure the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES):

- Encryption keys should be changed from default at installation and are changed anytime anyone with knowledge of the keys leaves the company or changes positions.
- SNMP community strings on wireless devices should be changed.
- Passwords/passphrases on access points should be changed.
- Firmware on wireless devices should be updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2).
- Other security-related wireless vendor defaults should be removed.

**PCI DSS 4.1.1** – Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.
- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

## 6 NETWORK SEGMENTATION

### 6.1 Merchant Applicability

Credit card data cannot be stored on systems directly connected to the Internet. For example, web servers and database servers should not be installed on the same server. A DMZ must be set up to segment the network so that only machines on the DMZ are Internet accessible.

#### **PA-DSS Requirements Reference:**

**9.1** The payment application must be developed such that the database server and web server are not required to be on the same server, nor is the database server required to be in the DMZ with the web server, per PCI DSS version 1.2 1.3.2.

## 7 SECURE REMOTE SOFTWARE UPDATES

### 7.1 Merchant Applicability

Sage Payment Solutions securely delivers remote payment applications by high-speed connections. Merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below.

For high-speed connections, updates are received through a firewall or personal firewall, per PCI DSS 1.

- Customers are recommended to use a firewall or a personal firewall product if computer is connected via VPN or other high-speed connection. In order to enable the operation of the update application, the end-user must only configure their firewall to provide outbound connections on the https standard port 443.

### 7.2 Personal Firewall

Any "always-on" connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product, per PCI DSS 1.3.9. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

### 7.3 Remote Update Procedures

The Sage Exchange desktop application is updated via published patches made available on the install web site. There are two ways in which these patches can be applied to existing installations.

- **Automated Update** – The automated update runs every hour starting from the time the Sage Exchange application is started. In the event a new version of the Sage Exchange becomes available the Sage Exchange will prompt the user to download the update. The user can either accept and download the update or decline and download the update later. After an update is downloaded the user is prompted to restart the Sage Exchange to apply the update. The user can either accept and restart the Sage Exchange or decline and the next time the Sage Exchange is started the update will be applied.
- **Manual Update** – A manual update check can be started by right clicking the Sage Exchange icon in the taskbar and selecting "Check For Updates". In the event a new version of the Sage Exchange is detected the Sage Exchange will prompt the user to download the update. The user can either accept and download the update or decline and download the update later. After an update is downloaded the user is prompted to restart the Sage Exchange to apply the update. The user can either accept and restart the Sage Exchange or decline and the next time the Sage Exchange is started the update will be applied.

#### **PA-DSS Requirements Reference:**

**10.1** If software updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on modem only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or personal firewall product to secure "always-on" connections, per PCI DSS version 1.2 1 and 12.3.9.

## 8 REMOTE ACCESS

### 8.1 Merchant Applicability

If Sage Exchange can be accessed remotely, all network connectivity should be performed using two-factor authentication per PCI DSS requirement 8.3. Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

### 8.2 Remote Access Software Security Configuration

Implement the following applicable security features for all remote access software used by the merchant, reseller or integrator:

- The default settings in the remote access software need to be changed.
- Only connections from specific (known) IP/MAC addresses need to be allowed.
- Strong authentication and complex passwords for logins need to be used according to the following PCI DSS requirements:

**PCI-DSS 8.1** - All users must have a unique username for access to system components.

**PCI-DSS 8.3** - Incorporate two-factor authentication for remote access.

**PCI-DSS 8.5.8** - Generic user IDs and accounts are disabled or removed. Shared user IDs for system administration activities and other critical functions cannot exist.

**PCI-DSS 8.5.9** - Require users to change passwords at least every 90 days.

**PCI-DSS 8.5.10** - Require passwords to be at least seven characters long.

**PCI-DSS 8.5.11** - Require passwords to contain both numeric and alphabetic characters.

**PCI-DSS 8.5.12** - Require that new passwords cannot be the same as the four previously used passwords.

**PCI-DSS 8.5.13** - Require that a user's account is locked out after not more than six invalid logon attempts.

**PCI-DSS 8.5.14** - Require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account.

**PCI-DSS 8.5.15** - System/session idle time out features have been set to 15 minutes or less.

- Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks, according to PCI DSS Requirement 4.1

**PCI DSS 4.1** - Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

- Account lockout needs to be enabled after six failed login attempts according to PCI DSS Requirement 8.5.13.
- The system needs to be configured so that a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Logging functions need to be enabled.
- Access to customer passwords needs to be restricted to authorized reseller/integrator personnel.
- Customer passwords need to be established according to the following PCI DSS Requirements:

**PCI-DSS 8.1** - All users must have a unique username for access to system components.

**PCI-DSS 8.2** - Users are authenticated using a unique ID and password.

**PCI-DSS 8.4** - Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

**PCI-DSS 8.5** - Ensure proper user authentication and password management for non-consumer users and administrators on all system components.

**PCI-DSS 8.5.1** - Control addition, deletion and modification of user IDs, credentials and other identifier objects.

**PCI-DSS 8.5.2** - Verify user identity before performing password resets.

**PCI-DSS 8.5.3** - Set first-time passwords to a unique value for each user and change immediately after the first use.

**PCI-DSS 8.5.4** - Immediately revoke access for any terminated users.

**PCI-DSS 8.5.5** - Remove/disable inactive user accounts at least every 90 days.

**PCI-DSS 8.5.6** - Enable accounts used by vendors for remote maintenance only during the time period needed.

**PCI-DSS 8.5.7** - Communicate password procedures and policies to all users who have access to cardholder data.

**PCI-DSS 8.5.8** - Generic user IDs and accounts are disabled or removed. Shared user IDs for system administration activities and other critical functions cannot exist.

**PCI-DSS 8.5.9** - Require users to change passwords at least every 90 days.

**PCI-DSS 8.5.10** - Require passwords to be at least seven characters long.

**PCI-DSS 8.5.11** - Require passwords to contain both numeric and alphabetic characters.

**PCI-DSS 8.5.12** - Require that new passwords cannot be the same as the four previously used passwords.

**PCI-DSS 8.5.13** - Require that a user's account is locked out after not more than six invalid logon attempts.

**PCI-DSS 8.5.14** - Require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account.

**PCI-DSS 8.5.15** - System/session idle time out features have been set to 15 minutes or less.

**PCI-DSS 8.5.16** - Not applicable. No database is used.

## 9 ENCRYPTING NETWORK TRAFFIC

### 9.1 Transmission of Cardholder data

Sage Exchange v1 payment application uses SSL v3.0 for transmission of cardholder data over Internet.

Merchants must use encryption, such as SSL/TLS or IPSEC, for transmission of cardholder data over public networks, per PCI DSS 4.1.

### 9.2 Email and Cardholder data

Sage Exchange does not natively support the sending of email. As per PCI DSS requirement 4.2, cardholder data should never be sent unencrypted via email.

### 9.3 Non-Console administrative access

The Sage Exchange v1 payment application does not have any administrative accounts. There is no cardholder data stored by Sage Exchange v1.

#### **PA-DSS Requirements Reference:**

**12.1** The payment application must use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and, internet protocol security (IPSEC)) to safeguard sensitive cardholder data during transmission over open, public networks, per PCI DSS 4.1.

Examples of open, public networks that are in scope of the PCI DSS are the Internet, Wi-Fi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

**12.2** The application must never send unencrypted PANs by e-mail.

**13.1** Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access, per PCI DSS 2.3.