InvenTrak POS (PosiTrak version 4.0)

PA DSS Implementation Guide

Version 1.0 – May 12, 2010

CONFIDENTIAL INFORMATION

This document is the property of InvenTrak POS; 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 InvenTrak POS.

1 INTRODUCTION

The purpose of this Implementation Guide is to instruct merchants, resellers, and integrators on how to securely implement InvenTrak POS and how to ensure your network is secure and compliant with the PCI PA DSS standards.

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Requirements that InvenTrak POS covers will be explained, as well as any requirements outside of InvenTrak POS, that you and your network administrator will need to meet. While this guide will go over in general, the network requirements, it is not intended to be a complete installation guide. You will need to put in place the details as determined by you and your network administrator.

Warning
Following these guidelines does NOT make you PCI DSS compliant, nor does it guarantee your network's security.
It is your responsibility, along with your network administrator, to ensure that your hardware and network systems
are secure from internal as well as external intrusions.
InvenTrak POS makes no claims on the security of your network, nor of your level of being PCI DSS compliant.

Please refer to the PCI Security Standards Council's Requirements documentation for guidance on network security

Notice
This document supports the PosiTrak 4.0 version for Windows XP and Windows 7

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect Stored Data

4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

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

2.1 Merchant and Reseller/Integrator Applicability

It is both the merchant's and reseller's or integrator's responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previous versions of the Positrak POS software. It is the responsibility of Inventrak to provide a means to do this. Removal of this prohibited historical data is required for PCI DSS compliance.

In addition, it is the merchant's and reseller's or integrator's responsibility to provide instructions regarding purging of cardholder data after expiration of customer-defined retention period.

2.2 Secure Deletion Instructions

The following instructions can be used to securely delete prohibited historical data and to purge cardholder data after expiration:

No previous versions of Positrak POS software have ever stored sensitive authentication data, including cryptographic key material to encrypt cardholder data, thus when installing Positrak POS software, no PAN data will be in the database. There is no need for any further action on the part of customers, resellers, or integrators.

PA DSS Requirements Reference:

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 payment application.
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 payment application).
- How to remove historical data
- That such removal is absolutely necessary for PCI DSS compliance.

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:

- Collect sensitive authentication only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

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 exceeding the customer-defined retention period must be purged.
- A list of all locations where the payment application stores cardholder data
- **2.7** Securely delete any cryptographic key material or cryptogram stored by previous versions of the payment application. These are cryptographic keys used to encrypt or verify cardholder data.
- Include the following instructions:
- That cryptographic material must be removed.
- How to remove cryptographic material
- That such removal is absolutely necessary for PCI DSS compliance.
- How to re-encrypt historic data with new keys

3 PASSWORD CONTROLS

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.

3.2 Passwords

The following guidelines should be followed.

- Customers and resellers/integrators are advised against using default administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database). (PA DSS 3.1c)
- Customers and resellers/integrators are advised to assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts. (PA DSS 3.1c)
- Customers and resellers/integrators are advised to assign strong application and system passwords whenever possible. (PA DSS 3.1c)
- Customers and resellers/integrators are advised that changing "out of the box" installation settings for unique user IDs and strong passwords will result in non-compliance with PCI DSS. (PA DSS 3.1c)
- Customers and resellers/integrators are advised how to create PCI DSS compliant, complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15. (PA DSS 3.1c)
- Customers and resellers/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. (PA DSS 3.2)

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

- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than 6 attempts
- Set the lockout duration to thirty minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

PA DSS Requirements Reference:

3.1 The "out of the box" installation of the payment application in place at the completion of the installation process must facilitate use of unique user ID's 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 DATA LOGS

4.1 Merchant Applicability

Currently, for PosiTrak version 4.0, there is no end-user, configurable, logging settings. All logging settings are hardcoded by Inventrak to conform to PCI DSS version 1.2 requirements 10.2.1-10.2.7 and 10.3.1-10.3.6. Logs must be enabled and disabling them will make it non-compliant with PCI DSS.

4.2 PCI DSS Guidelines for Logging

Implement automated audit trails for all system components to reconstruct the following events:

- All individual accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Record at least the following audit trail entries for all system components for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

PA DSS Requirements Reference:
4.2 Payment application must implement an automated audit trail to track and monitor access, per PCI Data Security Standard version 1.2.1; 10.2.1-10.2.7 and 10.3.1-10.3.6

5 PROTECT WIRELESS TRANSMISSIONS

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 1.2.1 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 DSS Requirements

Customers and resellers/integrators should install and configure perimeter firewalls between wireless networks and systems that store credit card data, per PCI DSS version 1.2.1; 1.2.3.

PA DSS Requirements Reference:

6.1 For payment application using wireless technology, the wireless technology must be implemented securely, per PCI DSS version 1.2.1; 1.2.3, 2.1.1 and 4.1.1.

6.2 For payment application using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

Payment applications using wireless technology must facilitate the following regarding use of WEP:

- 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 STORED DATA

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. The PosiTrak application is designed to be installed on an internal network segment. There is no need to establish a DMZ. The application has no web server functionality and has no requirement for the use of a network DMZ.

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; 1.3.2.

7 SECURE REMOTE SOFTWARE UPDATES

7.1 Merchant Applicability

The PosiTrak POS does not currently provide automated and/or remote software updates. Any updates to the application are performed manually. Typically, Inventrak will place software updates and patches on their website for downloading by their customers, resellers, or integrators. It is the responsibility of the customer, reseller, or integrator to download patches and updates and manually install them on their own systems running the PosiTrak POS application.

7.2 PCI DSS Requirements

If the payment application may be accessed remotely, customers and resellers/integrators must use a two-factor authentication (user ID and password and an additional authentication item, such as a smart card, token, or PIN), per PCI DSS version 1.2.1, 11.2.

8 REMOTE ACCESS

8.1 Merchant Applicability

The PosiTrak POS does not have any built-in remote access capabilities. The support staff at InvenTrak currently uses an application known as teamviewer.com in order to access customer systems remotely. All connectivity in this manner is performed using two-factor authentication per PCI DSS requirement 8.3. An ID and password are used as the first factor, and it is a requirement for the customer to furnish InvenTrak with ID and password, which allowing InvenTrak support staff the right to enter the customer's system. This physical act of providing an ID and password is the second factor for access. All remote access is initiated by the customer. At no time is it possible for InvenTrak to actually remotely access the system or running the application unless the customer has contacted InvenTrak support and requested such assistance.

In all cases, InvenTrak will:

- Whenever possible, InvenTrak will not gather data locally. Instead, InvenTrak will use remote troubleshooting applications that require express permission to access the computer, and which encrypts all traffic over HTTPS/SSL.
- InvenTrak will never request magnetic stripe data, card validation codes, PINs, or PIN block numbers.
- Data is only gathered with express permission, and only when required to resolve the specific problem.
- InvenTrak will never gather data that is not needed to solve the specific problem.
- Data is encrypted and stored in locations that have limited access.
- Data is deleted immediately after use.

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.

- Change default settings in the remote access software (for example, change default Passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication or complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8-8.15
- Enable encrypted data transmission according to PCI DSS Requirement 4.1
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirements 8.5.13
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed
- Enable the logging function
- Restrict access to customer Passwords to authorized reseller/integrator personnel
- Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5

PA DSS Requirements Reference:

11.2 If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism, per PCI DSS 8.3.

11.3 If vendors, resellers/integrators, or customers can access customers' applications remotely, the remote access software must be implemented securely, per PCI DSS 8.3.

9 ENCRYPTING NETWORK TRAFFIC

The payment application does not allow data transmission over public networks

9.1 Transmission of Cardholder data

The PosiTrak POS application does not transmit cardholder data over public networks. All information is send with SSL/TLS protocol.

9.2 Email and Cardholder data

PosiTrak POS application does not natively support or facilitate the sending of email containing cardholder data. As per PCI DSS requirement 4.2, cardholder data should never be sent unencrypted via email.

9.3 Non-Console administrative access

PosiTrak POS application does not natively support any non-console administrative access. If customers/resellers/integrators desire to facilitate secure non-console remote access, in all cases; remote access should be facilitated with software providing a secure tunneling connection such as SSH, VPN or SSL/TLS.

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, Wireless technologies, global system for mobile communications (GSM), and general packet radio service (GPRS).

12.2 The application must never send unencrypted PANs by end-user messaging technologies, such as e-mail, instant messaging, and chat.

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.

10 MAINTAIN DOCUMENTATION

This implementation guide, which covers all related requirements is available to all relevant payment application users (customers, resellers, and integrators). It is reviewed on an annual basis and updated as needed to document changes to the payment application and PA-DSS requirements.

Updates to the Implementation Guide can be obtained at www.retailcloud.com.

PA DSS Requirements Reference:

14.1 Develop, maintain, and disseminate a *PA-DSS Implementation Guide(s)* for customers, resellers, and integrators that accomplishes the following:

14.1.1 Addresses all requirements in this document wherever the *PA-DSS Implementation Guide* is referenced.

14.1.2 Includes a review at least annually and updates to keep the documentation current with all major and minor software changes as well as with changes to the requirements in this document.

14.2 Develop and implement training and communication programs to ensure payment application resellers and integrators know how to implement the payment application and related systems and networks according to the *PA-DSS Implementation Guide* and in a PCI DSS compliant manner.