TravStar1® POS System v9.01 Secure Implementation Guide

Guidance on how to securely implement the TravStar1 POS System into a PCI-DSS compliant retail environment

Fiscal Systems, Inc.
102 Commerce Circle
Madison, AL 35758
Office: (256) 772-8920
Help Desk: (800) 838-4549, press "3"
www.fis-cal.com

Document Version History			
Version	**Description**	**Approved**	**Date**
1.0	Initial Release for Version 9.00	KDS	15 JUL 09
1.1	Changed Patch and Update Instructions	KDS	11 NOV 09
1.2	Corrected Typographical Errors	KDS	22 APR 10
1.3	Annual Review	KDS	12 JUL 11
1.4	Verified reference web links are valid Updated web link on qualified QSAs Updated wireless guidelines	KDS	10 AUG 12

TravStar1® POS System v9.01
Secure Implementation Guide

1.0 PURPOSE

This secure implementation guide is provided to Fiscal Systems customers, resellers and support personnel with instructions, notes and pointers on how to implement and maintain the TravStar1 POS system v9.01 in a PCI-DSS compliant retail environment. This guide will be updated at least annually to incorporate changes in the TravStar1 POS system and the Payment Application Data Security Standard (PA-DSS) and Payment Card Industry PCI Data Security Standard (PCI-DSS). This guide is provided and maintained to comply with the requirements of the PA-DSS standard.

Following this guide does NOT make your retail environment PCI compliant, nor does it guarantee your network's security. It is your responsibility, along with your network administrator, to ensure that your software, hardware and network systems are secure from internal as well as external intrusions.

Fiscal Systems makes no claims on the security of your network, nor your compliance with the PCI Data Security Standard.

2.0 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Systems which process payment transactions necessarily handle sensitive cardholder account information. The Payment Card Industry, founded by American Express, Discover Financial Services, JCB, Mastercard Worldwide and Visa International, has developed security standards for handling cardholder information in a published standard called the PCI DSS. The security requirements defined in PCI DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted. The following high level 12 Requirements comprise the core of the PCI DSS:

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

The remainder of this document describes the essential guidance for implementing TravStar1 POS system in a PCI DSS compliant environment.

You can learn more about the PCI Security Standards Council and get a copy of the PCI DSS Standards at www.pcisecuritystandards.org.

3.0 INTRODUCTION TO TRAVSTAR1 POS SYSTEM

The TravStar1 POS system does not store full track data or sensitive authentication data (i.e. CVV, CVV2 or PIN blocks) after authorization. The TravStar1 POS system does not provide any access to or reporting of sensitive cardholder data, even by administrator accounts. All sensitive cardholder data is encrypted when stored and transmitted between POS system application modules with AES 256-bit encryption. Encryption keys are automatically generated and rotated by the POS system and cannot be accessed or modified by users or system developers. The encrypted sensitive cardholder data and expired encryption keys are automatically deleted by the POS system at appropriate intervals. No action on your part is required to enable these security features.

When determining the measures that need to be taken for PCI compliance, you need to review your entire system configuration:

- Your operating systems configuration and account controls
- Your network architecture and remote access to it
- Implementation of security software, such as antivirus and firewall applications
- Written policies and procedures for implementing and monitoring all of the above

Decisions on PCI compliance actions should take into account relevant factors that may be unique to your business, procedures and operating policies.

4.0 INSTALLING OR UPGRADING TO TRAVSTAR1® POS SYSTEM V9.01

Instructions for installing or upgrading the TravStar1 POS system can be found in the instructions supplied with your software. Those instructions, this secure implementation guide and a complete User Manual are available in electronic or printed formats from the Fiscal Systems Help Desk at (800) 838-4549, press 3. Electronic format document viewing requires Adobe Acrobat reader.

After successfully upgrading from a previous TravStar1 version, PCI DSS requires that you securely delete data files, log files and any back up files that might contain magnetic stripe data, card validation codes, PINs or PIN blocks. This mandatory PCI DSS requirement also includes files or data collected for troubleshooting (i.e data loaded in a spreadsheet). If you installed or made backups to other locations other than the default locations, you must locate and securely delete the files in alternate locations as well.

File types to Securely Delete in POS and OPT terminals at C:\Program Files\Fiscal

*.tsr	*.bak	*batch.dat	*.gzip
cauth.	cmedia.dat	rcmedia.*	*.tar
pmedia	*.comm	receipt.*	*.rar
ej*	*.prn	*.zip	
*.vdf	pch.*	*.tgz	

File types to Securely Delete in Site Controller at \home\ccl\ccl

tfc.dat	dbatch*	ADSrev*	dpfallbk.dat
rbatch*	cbatch*	ADS_fb.new	bpfallOK.dat
bbatch*	$ADSfallbk.dat	bpfallbk.dat	*.comm

Note: These are default filenames and extensions, if you specified something different at any time, delete those files as well.

Standard file deletion tools in the Windows and Linux operating systems do not meet the secure deletion standard specified in PCI DSS. You must obtain and use a secure

deletion application for this purpose or utilize a qualified third party that provides this service. Fiscal Systems recommends the following secure deletion applications. They are available as free downloads from the Internet. Support for their use is available from the Fiscal Systems Help Desk at (800) 838-4549, press 3.

POS and OPT Terminal (Windows operating system)

SDelete (Secure Deletion)

Download from:
http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

Directions:
SDelete is a command line utility that takes a number of options. In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk. ***SDelete*** accepts wild card characters as part of the directory or file specifier.

Usage:
sdelete [-p passes] [-s] [-q] <file or directory>
sdelete [-p passes] [-z|-c] [drive letter]

-c	Zero free space (good for virtual disk optimization).
-p	Specifies number of overwrite passes.
-s	Recurse subdirectories.
-q	Don't print errors (quiet).
-z	Cleanse free space.

Examples:

1. Removing specific files. To remove void data files (*.vdf) on the POS:

   sdelete -p 7 -s C:\Program Files\Fiscal*.vdf

2. Wiping free space on drive to remove traces of files that were previously deleted by insecure methods.

   sdelete -p 7 -z -c C:

Site Controller (CCL) (Linux operating system)

BCWipe

Download from:
http://www.jetico.com/bcwipe_unix.htm

BCWipe for UNIX is designed as UNIX-style command-line utility.

Usage:
bcwipe [-fhMv] [-m mode] [-n delay] FILE1 [FILE2]

-f Force wipe files with no write permissions. Also suppress interactive mode (-i switch)
-F Wipe free space on specified filesystem
-h Display help screen and exit
-md US DoD 5200.28 seven pass extended character rotation wiping
-v Run in verbose mode

Note: Display the help screen (bcwipe –h) to see a full list of available commands.

Examples:

1. Removing specific files. To remove batch files (batch*) on the Site Controller:

   bcwipe -mdvf rbatch*

2. Wiping free space on drive to remove traces of files that were previously deleted by insecure methods.

   bcwipe -Fmdv /home/ccl/ccl

5.0 SECURE ACCESS CONTROL

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process. Additionally any default accounts provided with operating systems and/or devices should be removed/disabled/renamed as possible, or at least should have PCI DSS compliant complex passwords and should not be used. Examples of default administrator accounts include "administrator" (Windows) and "root" (SuSE Linux).

PCI DSS requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

PCI DSS user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

Each cashier must have a unique cashier ID and password so their activities on the POS system can be accounted for and tracked. Cashier passwords are stored as a salted hash so they cannot be recovered if forgotten. If a cashier ID and password are forgotten, a new set must be created.

All unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, FTP server, HTTP server, etc.) should be disabled on each POS terminal running the TravStar1 POS System. Services can be disabled from **Control Panel**, **Administrative Tools**, **Services**.

The System Restore function of Windows operating system must be turned off. First, log onto the POS terminal with Adminstrator privileges. Right click **My Computer**, and then click **Properties**. In the **System Properties** dialog box, click the **System Restore** tab. Click to select **Turn off System Restore** check box. Then click **OK** when you receive the message "You have chosen to turn off System Restore. If you continue, all existing restore points will be deleted, and you will not be able to track or undo changes to your POS terminal. Do you want to turn off System Restore?" The System Properties dialog box will close in a few moments. Repeat this process for each POS terminal.

The POS terminal should never be used to host a public FTP or HTTP (Web) server. Protocols and Ports can be disabled from the Windows Firewall and the Hardware Firewall.

6.0 BUILDING AND MAINTAINING A SECURE NETWORK

Consistent with network security best practices, the PCI DSS requires that your network:

- Be protected from unauthorized traffic using a firewall
- Have antivirus software installed and updated regularly
- Is regularly updated with the latest operating systems and network software patches to keep your system current

The following guidelines are general in nature. It is recommended that you consult a qualified network administrator to review your particular network setup for purposes of implementing the best protective measures for your unique situation.

Build a firewall configuration that:

- Denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment,
- Restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks include:
  - Restricting inbound internet traffic to IP addresses within the DMZ (ingress filters)
  - Not allowing internal addresses to pass from the internet into the DMZ
  - Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)
  - Outbound Internet access from the trusted segment must be limited to required and justified ports and services.
  - Placing the database in an internal network zone, segregated from the DMZ
  - Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment and denying all other traffic
  - Employ an encryption method with at least 128-bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as AES) on outbound Internet access or Internet accessible DMZ network segments to comply with PCI DSS requirements
  - Securing and synchronizing router configuration files
  - Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

- Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet which is also used to access the company network

If your implementation will transmit sensitive card holder data over open, public network, such as a broadband Internet connection, you must employ strong cryptography and security protocols such as secure socket layer (SSL) and Internet Protocol Security (IPSEC) to safeguard the sensitive cardholder data.

7.0 REMOTE NETWORK ACCESS

To comply with PCI DSS requirements, you must implement two factor authentication for remote access granted to the network for employees, administrators and third parties. Employ network security technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

When utilizing remote network access software you must implement the following security features:

- Change default settings in the remote access software (for example, change default passwords)
- Use unique passwords for each user of remote network access
- Allow connections only from specific (known) IP and MAC addresses
- Use strong authentication or complex passwords for logins
- Enable encrypted data transmission
- Enable account lock out after a certain number of failed login attempts
- Configure the system so a remote user must establish a VPN connection via a firewall before access is granted
- Enable the logging function
- Restrict access to passwords to authorized reseller/support personnel
- Establish passwords according to PCI DSS requirements
- Rotate pre-shared keys and certificates at least annually

If you use remote access to perform non-console administrative access, you must use SSH, VPN or SSL/TLS encryption and the above security features to comply with PCI DSS requirements.

8.0 WIRELESS NETWORKING

If you deploy wireless networking devices on the same network as the POS system, consult your networking equipment vendor documentation and online resources carefully for the optimum security configuration.

To comply with PCI DSS requirements when using wireless networks:

- Install and configure a firewall on each POS terminal and site controller
- Modify the default wireless equipment settings, including:
  - Change default encryption keys
  - Change default service set identifier (SSID)
  - Change default passwords
  - Change default SNMP community strings
  - Disable SSID broadcasts
  - Enable strong cryptography such as WiFi protected access (WPA or WPA2) technology for encryptions and authentication
- If cardholder data is transmitted with a wireless network, encrypt the transmission with strong cryptography such as WPA or WPA2 technology, IPSEC VPN, or SSL/TLS. Never rely on WEP to protect sensitive cardholder data and access to the wireless LAN.

You can learn more about wireless network installations in the PCI Security Standards Council information supplement, "PCI DSS Wireless Guidelines." You can download a copy at www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf.

9.0 MAINTAINING A VULNERABILITY MANAGEMENT PROGRAM

Updates to the TravStar1 POS system are released periodically to add or enhance functionality and fix identified defects or vulnerabilities. If there are changes to the PCI DSS requirements or in related POS features, the updates will include updated electronic documentation, including this implementation guide to facilitate your compliance. Check with the Fiscal Systems Help Desk at (800) 838-4549, press 3, periodically for updates.

As a software development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of Point of Sale systems. We do this by subscribing to relevant data feeds and news services which inform us of potential security issues.

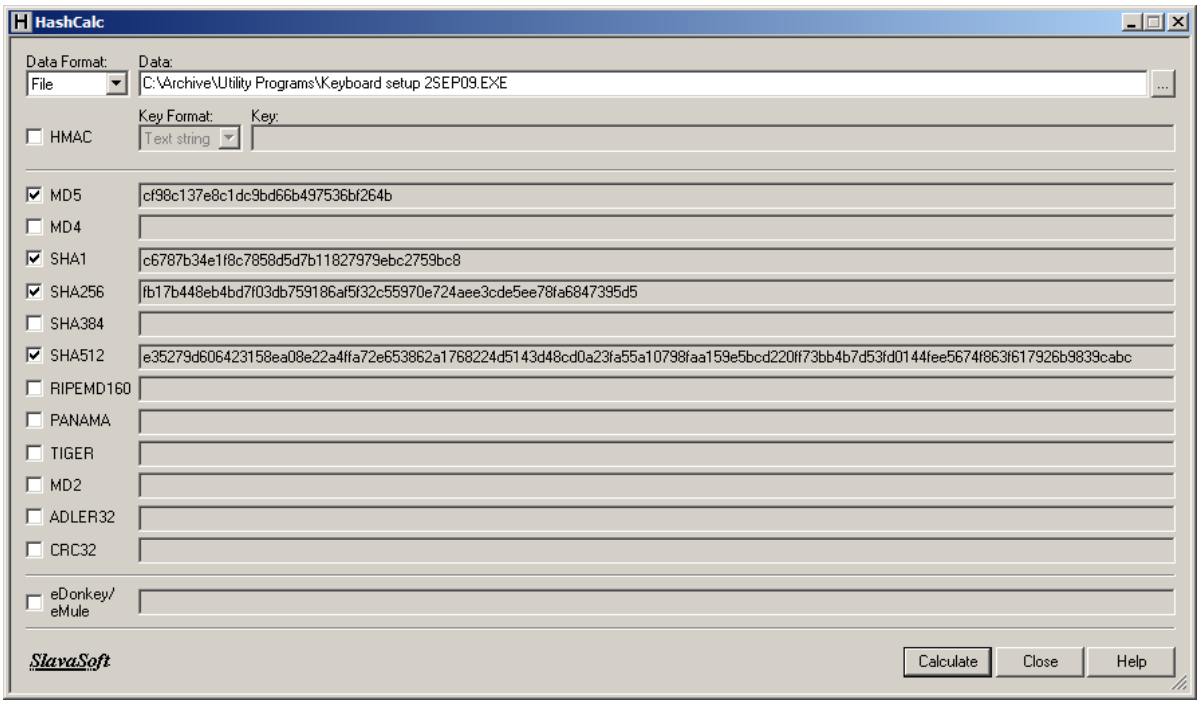
We recommend that your systems (Linux and Windows operating systems) be maintained automatically by using an automatic update service to download security patches daily. Refer to section 14.0, Operating System Information, for more information on operating system support.

If security vulnerabilities are identified not covered by these automatic updates, we work to develop and test a patch that helps protect the TravStar1 POS system against the specific, new vulnerability. We attempt to publish a patch within 30 days of the identification of the vulnerability. We will then contact merchants to notify them of the availability of the patch. Typically, merchants are expected to respond quickly to test and install available patches within 30 days.

Fiscal Systems does not remotely connect to your network without your permission, to "push" POS system updates to you. You have complete control over when and how POS system updates are installed on your system.

We deliver software and patches via secure remote access to customer networks. We maintain a secure connection to your POS system by use of SSH or SFTP, which ensure that all communication is encrypted and the legitimate identity of your system and ours is verified. Refer to section 7.0, Remote Network Access, for more information on secure remote network access.

The release notes for software and patches include MD5, SHA1, SHA256 and SHA512 hashes to verify the integrity of the file. Fiscal Systems recommends "HashCalc" as a hash calculator available as free download from the Internet. Download it at http://www.slavasoft.com/hashcalc/index.htm. Hash values for software and patches and support for using HashCalc is available from the Fiscal Systems Help Desk at (800) 838-4549, press 3.



Install antivirus and spyware detection software and keep it up to date. These software products are designed to detect and remove malicious software code that typically is installed without your knowledge or permission for the purpose of damaging files or data, intercepting sensitive cardholder data, or tracking your computer activities.

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every retail merchant should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed. PCI Security Standards Council trains, tests and certifies organizations and individuals to assess and validate adherence to PCI Security Standards. A current list of Qualified Security Assessor (QSA) companies is available on the Internet at….

  www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

10.0 Secure Remote Updates

Fiscal Systems does not force automatic updates of the TravStar1 POS system. You have complete control over when and how POS system updates are installed on your system. If you allow POS system software updates to be deployed remotely, you must create a policy for critical employee-facing technologies that contains the following security features to comply with PCI DSS requirements:

- Explicit management approval to use the devices
- All device use is authenticated with two-factor authentication, such as a username and password and a physical authentication item (token or certificate)
- List of all devices and personnel authorized to use the devices

- Labeling of devices with owner, contact information and purpose
- Define acceptable uses for the technology
- Establish acceptable network locations for the technology
- Establish a company-approved products
- Require an automatic disconnect of sessions after a period of inactivity
- Require the activation of modems used by vendors only when needed by vendors, with immediate deactivation after use
- Prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media.
- Prohibit cut and paste and print functions during remote access
- Require the use of a personal firewall product if computer is connected via VPN or other high-speed connection to secure these "always on" connections to comply with PCI DSS requirements

11.0 LOGGING AND AUDITING

Even though POS system logs cannot be configured to contain sensitive cardholder data, it is encouraged to set logging configurations to keep logs only for the number of days necessary to support the stores. PCI DSS requirements state users must employ a backup procedure that archives and stores all security logs for at least one year.

Sites should implement automated audit trails for all system components to reconstruct the following events:

- All actions taken by and 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.

For more information on PCI requirements for security log settings, please refer to the PCI DSS standard.

12.0 Internet Applications

In order to meet the requirements of PCI DSS, sensitive cardholder data cannot be stored on a computer connected to the internet. The TravStar1 POS system does not provide internet services, and does not require that any internet applications reside on the computer containing cardholder data. Software that provides internet services (such as a web server or FTP server) must never be run on the same computer as the TravStar1 POS system.

13.0 System Troubleshooting

When troubleshooting cardholder problems, PCI DSS requires that retail merchants, resellers, integrators and support personnel:

- Collect the minimum amount of sensitive data necessary to solve a specific problem.
- Store sensitive data in specific, known locations with limited access.
- Sensitive authentication data must be encrypted while stored.
- Securely delete sensitive data if stored electronically or physically destroy (e.g. cross shredding) printed sensitive data immediately after use. Do not simply discard the sensitive data.

If you transmit or share any sensitive cardholder data outside of the POS system to a third party, such as a Front End Processor, corporate bookkeeping department or technical advisor, it is your responsibility to understand and follow the PCI Data Security Standard requirements for the security of such transmissions.

The POS System does not have a facility to email sensitive cardholder data. If you need to email or otherwise transmit sensitive cardholder data, it must be transmitted only in an encrypted format, such as SSL.

14.0 Operating System Information

The current version of the TravStar1 POS system applications v9.01 are developed and deployed on the Windows and SuSE Linux operating systems.

To comply with PCI requirements, a validated application must execute from a system that is supported by the manufacturer, to include up-to-date security related patches and enhancements.

If you are unsure of which operating systems are valid, please reference the current operating system manufacturers page.

Example for Microsoft:

http://www.microsoft.com/windows/lifecycle/default.mspx

Example for SuSE Linux:

http://support.novell.com/linux/psdb/byproduct.html

15.0 Reseller and Support Personnel Training

Training is available to resellers and support personnel to ensure that they can implement and maintain the TravStar1 POS system in a PCI DSS compliant retail environment. Training is available via updated documentation and custom training session under standard consultancy arrangements. Contact the Fiscal Systems Help Desk at (800) 838-4549 for more information on training requirements and available dates.

16.0 Reference

Payment Card Industry (PCI) Data Security Standard v1.2.1

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

17.0 Acknowledgements

Throughout this guide we provided links to Internet sites of providers of security related products, information, and industry organizations that can provide additional assistance with understanding the PCI DSS requirements. These links are provided for your convenience. Unless specifically stated, Fiscal Systems does not own, endorse or specifically recommend any of the products or vendors listed. Decisions on PCI compliance actions should take into account relevant factors that may be unique to your business, procedures and operating policies.