Travstar1 v11.01.0001

Secure Implementation Guide

Document Version History			
Version	**Description**	**Approved**	**Date**
1	Initial release of Travstar1 version 11.01.0001 under PCI-SSF standard	WB	10 Feb 23

Note: The following guide applies solely to those customers upgrading or receiving the Travstar1 system on the SUSE Linux Enterprise Server 15 SP3 operating system. Those continuing to use version 11 SP4, refer to the guide you received with your system.

When determining measures to be taken for PCI compliance, the best practice is 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 the above

Decisions impacting PCI compliance should consider relevant factors unique to your business, procedures, and operating policies.

1.0 Do not retain full track data, card verification code, or value

As Travstar1 does not store PAN or sensitive authentication data (i.e., CVV, CVV2 or PIN blocks) after authorization, any actions requiring such storage, temporary or otherwise, PCI DSS requires that retail merchants, integrators, and support personnel:

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

The POS System does not store any sensitive authentication data nor does it have a facility to email sensitive authentication data as part of the troubleshooting process.

The below locations are the only accessible areas in which partial PAN data is available. All PAN data is masked (Last four digits of the PAN) and defined as unreadable. It is not possible for any user to manipulate the readability of this PAN data. Masked PAN data is also available on customer receipts excepting the last four digits.

1. Point of Sale Terminals (POS) The current log is Poslog.dat and is located in C:\Program Files\Fiscal\. Logs archived by the application are named Poslog.XXXX where XXXX is the shift reset on the POS located in C:\Program Files\Fiscal\poslogs.

2. Site Controller (LSC) Travstar1 The current log is syslog.dat and is located in /home/sitecon/sc. Logs archived by the application are named syslogXX.dat where XX=1-99. The archived logs are located in /home/sitecon/sc/logs.

3. Credit Card Library (CCL) The current log is ccllog.dat and is located in /home/ccl/ccl. Logs archived by the application are named ccllog.datXX where XX=1-99. The archived logs are located in /home/ccl/ccl/logs.

4. The Linux Payment Terminal (LPT) log is named lptlog.dat and is located in /home/lpt. Logs archived by the application are named SyslogXX.dat where XX=1-99. The archived logs are located in /home/lpt/logs.

As previously stated, the system does not store cardholder data beyond the masked PAN. Therefore, user access audit requirements are not applicable.

If you transmit or share any 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 PCI requirements for the security of such transmissions.

2.0 Protect stored cardholder data

The below is designed to meet all associated PCI-DSS requirements for payment applications as well as to protect the system against both local and outside threats. At the highest level of importance, the PAN is displayed masked (first six and last four digits) by default in all instances.

Travstar1 automatically manages the encryption keys used to secure sensitive authentication data and PAN data during the preauthorization phase using AES-256 bit, no actions from the customer are required.

During the transaction process, masked PAN data is stored in the form stated above (only the first six and last four digits). This results in the inclusion of the same masked data appearing in the log files.

This masked PAN stored per each transaction enters Travstar1 allocated to a temporary buffer which receives a unique encryption key. Upon completion of the authorization, this buffer containing the masked PAN is allocated to a block of memory which is subsequently deleted by the AESDecryptData function hardcoded to the system. Said deletion function achieves this via a process during which the data is passed through a 7-step process. Binary 0s, binary 1s, randomized bits are overwritten and then run through again. Between each pass of writes, the file data is flushed and synced to disc storage. As this process is proprietary, it cannot be fraudulently duplicated or accessed whatsoever. Furthermore, any sensitive items contained within the Credit Card Library (CCL) module used during the authorization phase is entirely inaccessible regardless of user account rights.

No sensitive authentication data or any full PAN is stored after a transaction is complete.

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

At a minimum, the following audit trail entries for all system components for each event must be recorded:

- 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.

3.0 Provide secure authentication features

PCI DSS requires that access to all systems in the payment-processing environment, whether non-administrative or otherwise, be protected through use of unique users and complex passwords. Additionally, any default accounts provided with operating systems and/or devices should be removed/disabled/renamed as possible and should not be used. Examples of default administrator accounts include “administrator” (Windows) and “root” (SuSE Linux). PCI-DSS requirement 8 covers these requirements.

Each location is responsible for maintaining their own unique passwords as Travstar1 does not maintain these. Passwords must be managed at the operating system level. It should be noted, therefore, the respective operating system stores user account names and passwords. Each vendor approaches securing this data with proprietary methods. All levels of encryption, utilization of multiple locations in which usernames and passwords are never stored together, and the prevention of unauthorized access are at the highest levels of security.

Users are encouraged to implement an additional level of user account security by never using the same account passwords in multiple systems. Administrators should make it a practice to utilize Microsoft’s Local Administrator Password Solution (LAPS) or similar service to automate this practice. LAPS is inherently compatible and acts as a password manager, generating unique local Administrator passwords for each system.

For **Non-administrative** users:

PCI compliance requires the following password complexity:

- 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 cannot be the same as the last 4 passwords
- If an incorrect password is provided 6 times the account should be locked out
- Account locks out duration should be at least 30 minutes 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 user 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. Under no circumstances are logins, credentials, or any further method of access to be shared between individuals.

PCI requirements further dictate all users be assigned specific roles and responsibilities. Such roles must be documented and maintained by a designated administrator. The assignments must also correlate to the level of access granted with each unique login.

For **Administrative** users:

Any account with access to the Operating System or hardware on which the POS console resides i.e., an administrative account used for Windows purposes but not Travstar1, must be demonstrably prevented from accessing the console. Under no circumstances is the console to be subject to potential access by an Operating System login.

If any such access is required, it is recommended Fiscal Systems support is contacted beforehand to advise and/or assist where prudent. Fiscal Systems does not recommend nor require such accounts be necessary.

The Travstar1 console is to be accessed only through unique and authorized accounts only further secured with Multi Factor Authentication. All such non-console access needs must be routed to Fiscal Systems Support to ensure secure and compliant methods listed in section 10.

4.0 Log payment application activity

Logs should not be disabled and doing so will result in non-compliance with PCI DSS.

Travstar1 takes advantage of centralized logging in which all application activity is consolidated to a specific location within each respective unit.

Logs are stored in regular text files and can be exported by any third party centralize logging solution by pointing it to the file path for each log.

Names and locations of POS System application logs:

Travstar1 by default will store logs in the files listed below, these logs are enabled by default after the installation process and automatically configured to meet PCI-DSS requirements. No actions are required by the customer.

Transaction logs stored on the Point of Sale (POS), Credit Card Library (CCL), and Site Controller (LSC) are removed or overwritten as listed below. These specifications represent the default state of these processes as shipped. It should be noted logs stored on the POS are the only such items removed based on timeframe. All others are overwritten based upon the number of entries.

1. Point of Sale – The default retention period for transaction logs is 15 days

2. Site Controller – The aforementioned syslogs stored on the LSC are overwritten based upon the file structure syslogXX.dat where XX=1-99. Once the 99th log is entered, the next entry overwrites the previous syslog01.dat and subsequent entries continue as such

3. Credit Card Library – The same process governing log retention on the LSC apply to the CCL as well. Once the 99th entry limit is reached, entries overwrite beginning with 01 and continuing

4. Linux Payment Terminal – As is the case with LSC and CCL logs, entries are stored numbering 1-99 and overwrite as the limit is reached

5.0 Versioning

The below represents the standard Travstar1 versioning method as it is released across all newly deployed or updated systems. To facilitate the support of individual sites, a unique identifier unrelated to the system version will be applied to customer installations which will also be visible.

Fiscal Systems, Inc. publishes Travstar1 versions using the following methodology. Three elements separated by a literal period, the third of which includes a dash allowing for further specificity. The result is the format XX.XX.XX-XXXX and is defined as follows:

1st element (Numeric) - This is the major version number and would represent a significant enhancement or functionality change. This can include changes impacting security of cardholder data, or high impact changes affecting PCI compliance.

2nd element (Numeric) - This is the minor version number and would represent a minor enhancement to the application. This can include low impact changes affecting PCI regulations but do not impact security.

3rd digit (Numeric) - This is primarily the patch or revision number and is represented by the digits preceding the dash. Absent changes to the previous elements, this value will be the most common indicator separating current and previous versions. When this is incremented, the release could address defects in previous patches or discovered minor deficiencies not affecting application functionality or security. As such it will not meet the criteria of fields 1 and/or 2 therefore no changes in the third element impact PCI-DSS requirements in any way.

The remaining digits following the dash represent the build associated with the preceding Patch value. This value will adjust in varied configurations as each Patch is unique and may require non-uniform build identifiers.

All upgrades, updates, patches, or changes to the product will result in an updated version number and will not be conducted without appropriate notification given and acknowledgement provided.

6.0 Protect wireless transmissions

Travstar1 is not developed for use with wireless technology. However, 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:

- Change all wireless default encryption keys, passwords, and SNMP community strings upon installation.

- Change wireless encryption keys, passwords, and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.

- Install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

- Use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.

7.0 Test payment applications to address vulnerabilities and maintain payment application updates

The Travstar1 application v11.01.01-0001 validated under PA- DSS 3.2 will remain in place until such a time as any system is updated or a new deployment is executed. The application supports the following operating systems:

POS	Windows POS Ready 7 SP1, Windows 10 Enterprise LTSC
LPT	SUSE Linux Enterprise Server 15.3
SC	SUSE Linux Enterprise Server 15.3
CCL	SUSE Linux Enterprise Server 15.3

The following software components are required (These are included with the software and maintained by Fiscal Systems, Inc., no action is requested by customer):

OpenSSL version 3.0 Visual C++ 2008 Sp2

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.

Fiscal Systems does not force automatic updates of the Travstar1 System. You have complete control over when and how POS system updates are installed on your system. These parameters must be communicated to Fiscal Systems Support.

The Fiscal Systems, Inc. Support group deploys software updates via AES 256-bit encrypted VPN on behalf of clients, by connecting to the Travstar1 using SSH, SCP, and SFTP. This remote connection in only activated when needed and is immediately deactivated after use. Remote connections are further protected by Multi Factor Authentication challenges prior to remote personnel receiving individual permissions to connect to outside networks. This function is implemented and managed by Fiscal Systems and is universal for all networks.

Regardless of the nature of the release, a thorough code review is conducted and any items displaying sensitive information are scrubbed.

If there is ever a need to roll code back to a previous version, contact the Support group and it will be promptly rolled back. 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 requirements:

- Explicit management approval to use the devices
- All device use is authenticated with multi-factor authentication, such as a username and password and a physical authentication item (token or certificate) Travstar1
- 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 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 requirements.

Updates to the Travstar1 are released periodically to add or enhance functionality and fix identified defects or vulnerabilities. If there are changes to the PCI requirements or in related POS features, we can provide you with updated documentation upon request.

Check with the Fiscal Systems Help Desk at (800) 838-4549, press 3, 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, network infrastructures, and various

development software to include techniques and vulnerable data sources. We do this by subscribing to relevant data feeds and news services, communications with industry partners, and dedicated services which provide information and early warning for potential security issues.

While Travstar1 is a proprietary software, it is subject to the proper use of the Windows environment on which it runs. Of note is a potential vulnerability to the system involving the use of paging files. Windows utilizes paging files, or swapfiles, to create temporary storage space on a hard drive when RAM resources are depleted. In order to mitigate the potential misuse of this feature, virtual memory allocation should not be altered.

We recommend that your operating system be maintained automatically by using an automatic update service to download security patches daily. The POS and Manager's Workstation reside on the Windows 10 platform. It is highly recommended regular updates be applied as issued by Microsoft. Notification will be given of available updates by the aforementioned organization as well as instructions on how they are to be applied.

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 authentication 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

8.0 Facilitate secure network implementation

Consistent with network security best practices, the PCI-SSC 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 network setup for purposes of implementing the best protective measures for your unique system deployment and topology.

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 TLS 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.

9.0 Cardholder data must never be stored on a server connected to the Internet

The POS system as delivered does not store cardholder data storage. In turn, Travstar1 does not require an outward facing endpoint such as a webserver or any asset residing on a DMZ. Furthermore, as Travstar1 does not in any capacity require a storage component to operate outside the boundaries of its current configuration, no outside storage option elected by the customer should in no way reside on the same.

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.

Alongside the prevention of the above vulnerabilities, Travstar1 requires the below configuration to include ports, services, destinations, and components. Use this information to configure protocols and ports appropriately.

Port: 4559-4589 TCP	**Source: POS**	**Destination: Site controller**
Port: 7777 TCP	**Source: LPT**	**Destination: Site controller**
Port: 5555-5585 TCP	**Source: POS**	**Destination: Managers Workstation**
Port: 5432 TCP	**Source: POS**	**Destination: Managers Workstation**

Port: 50001 TCP	**Source: POS**	**Destination: additional POS (if applicable)**
Port: 9100 TCP	**Source: POS**	**Destination: 80 Column Printer**
Port: 9100 TCP	**Source: Managers Workstation**	**Destination: Report Printer**
Port: 22 TCP	**Source: POS LAN Segment**	**Destination: POS LAN Segment**
Port: 2011-2014 UDP	**Source: Site controller**	**Destination: WAN**
Port: 53 UDP	**Source: Site controller**	**Destination: WAN**
Port: 443 HTTPS	**Source: Site Controller**	**Destination: WAN**
Port: 3555-3585 TCP	**Source: POS**	**Destination: Site controller**

All other insecure services and protocols (e.g., NetBIOS, file-sharing, FTP server, HTTP server, etc.) should be disabled on each POS terminal running the Travstar1 System. Services can be disabled from Control Panel, Administrative Tools, Services.

10.0 Facilitate secure remote access to payment applications

All networks, POS systems, Site Controllers, and business-owned systems must be segmented and/or otherwise secured from outside access. This includes any wireless networks available for guest use.

If any wireless or wired network is configured such that it can view systems within the scope of PCI-DSS, it is considered within scope and unauthorized access is to be prevented in all circumstances.

To comply with PCI requirements, you must implement multi-factor authentication for remote access granted to the network for employees, administrators and third parties.

Fiscal-Systems Customer Support personnel are required to authenticate via unique usernames, passwords and multi-factor authentication facilitated by DUO. This ensures personnel are dually authenticated prior to accessing tools required to connect to all customer networks.

TravsStar1 System does not directly facilitate any type of remote access that originates from outside the customer environment.

Remote access to your environment by Fiscal Systems customer support begins with a per-session unique challenge to each individual attempting to access any system therein regardless of method used i.e. SSH, RDP, etc. These processes are implemented, managed, and enforced by Fiscal Systems.

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 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 support personnel
- Establish passwords according to PCI DSS requirements
- Rotate pre-shared keys and certificates at least annually

If remote access is used to perform non-console administrative access, you must use SSH, VPN or TLS encryption and the above security features to comply with requirements. Fiscal Systems in its capacity to remote to your network utilizes the MFA policies created within our domain attached to a support individual's specific credentials. This ensures that remote access is logged and enforced on a per user per session basis prior to an attempt to make remote contact. The process is facilitated by the VPN client installed on each support workstation and the local firewall to prevent additional complications brought on by utilizing additional equipment.

To further extend efforts to eliminate potential vulnerabilities, the login challenge process is enforced prior to personnel receiving any access whatsoever to resources attached to enabling connections to your network. The outcome is remote support is authenticated prior to accessing your network's specific remote solution.

Given the above process, specific ports must be configured to permit the encrypted traffic established by the VPN connection as directed

11.0 Encrypt sensitive traffic over public networks

The Travstar1 does not provide any access to or reporting of sensitive authentication data at any time during or after card authorization, even by administrator accounts. Only the masked PAN is accessible (Ex. 123456XXXXXX9112). All sensitive authentication data and PAN data is encrypted when stored during the preauthorization phase. It is also transmitted between POS system application modules and the payment processor with AES 256-bit encrypted payload. At no point does the system attempt to send data beyond the bounds of its components.

Travstar1 does not facilities sending PAN via end-user messaging technologies.

TLS 1.2 AES 256-bit or a VPN are the only supported methods of transmitting account data to the payment processor. 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 after authorization.

No action on your part is required to enable these security features.

12.0 Maintain a compliant Implementation Guide for customers, resellers, and integrators.

In the event an additional compliance related Implementation Guide is required, one can be requested through Fiscal Systems support. In the event significant changes to the PCI-DSS requirements and/or the nature of the Travstar1 console also result in changes to this document, one will be forwarded and will be subject to the same level of acknowledgement. In the event there are changes to system components resulting in an updated version of the application, a subsequent Implementation Guide will be issued carrying the same acceptance procedures as the previous.

This guide should be kept for your records and accessible to requesting and appropriate entities or personnel.

13.0 Assign responsibilities for personnel, and maintain training programs for personnel, customers, resellers, and integrators.

PCI compliance requires formal training of all personnel with access to cardholder data as well as the systems which process such data. The PCI Security Standards Council provides materials and templates to conduct such training. No other source or service provider is recommended in this capacity.

Fiscal Systems may only advise as requested during the course of standard product support evolutions; however, this is not to be considered an authoritative interaction tantamount to meeting said standards.

The training materials, programs, and personnel responsible for overseeing this program must be formally assigned and documented as part of your compliance documentation.

Contact

If any of the above information requires clarification or for further information, contact Fiscal Systems support at _____

Acknowledgement

I have received, read, and understood the contents of the above guide as well as the described standards necessary to meet PCI requirements as written on the below date. I acknowledge the roles and responsibilities contained herein as well as those of Fiscal Systems, Inc. I further acknowledge that all responsibilities for meeting requirements set by the PCI Security Standards Council outside the as-delivered Travstar1 system rest within my organization.

Signed: _____

Date: _____

This document has been reviewed and approved by the below representatives of Fiscal Systems, Inc

_____	_____
Will Bradley Fiscal PCI Compliance	Date
_____	_____
Judise Lanier VP Product Strategy and Development	Date
_____	_____
Blake Beck VP Software Development	Date