# Travstar1 v10.01.02-XXXX_XXX

**Fiscal Systems, Inc.**
4946 Research Drive
Huntsville, AL 35805
Office: (256) 772-8920
Help Desk: (800) 838-4549, Option 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 | Annual Review<br>Corrected Typographical Errors | KDS | 22 APR 10 |
| 1.3 | Annual Review | KDS | 12 JUL 11 |
| 1.4 | Annual Review<br>Verified reference web links are valid<br>Updated web link on qualified QSAs<br>Updated web link for PCI wireless guidelines | KDS | 10 AUG 12 |
| 1.5 | Annual Review<br>Verified reference web links are valid<br>Added Log Review Instructions | KDS | 12 JUN 13 |
| 1.6 | Annual Review<br>Verified reference web links are valid | KDS | 16 JUN 14 |
| 1.7 | Annual Review<br>Verified reference web links are valid<br>Updated Business Address<br>Updated Secure Access Control<br>Added detailed Log Review Setup Instructions | NBJ | 30 MAR 15 |
| 1.8 | Added Software Versioning Methodology | NBJ | 14 OCT 15 |
| 1.9 | Added Required Ports/Services<br>Modified Log review Setup Instructions<br>Added Centralized Logging | NBJ | 19 OCT 15 |
| 2.0 | Updated Required Ports/Services<br>Updated Secure Remote Updates<br>Updated Auditing and Centralized Logging | NBJ | 02 FEB 16 |
| 2.1 | Updated Software Versioning Methodology | NBJ | 17 Feb 16 |
| 2.2 | Full Certification<br>Updated Software Versioning Methodology | BTH | 5 May 17 |
| 2.3 | Updated Introduction<br>Updated Remote Access to "Multi-factor"<br>Revised Version number<br>Updated "Travstar1 POS" to just "Travstar1 " for clarity. | BTH | 22 JUN 17 |
| 2.4 | Minor wording changes throughout for clarity<br>Adjusted Wording of PCI-DSS requirements to match PCI-DSS 3.2<br>Updated network connections to clearly define every connection<br>Updated references to stored cardholder data to state that it is only stored during preauthorization. | BTH | 02 AUG 17 |
| 3.0 | Final Changes for 3.2 Validation | BTH | 26 OCT 17 |
| 3.1 | Corrected version numbers, added supported operating systems, updated dates | BTH | 1 NOV 17 |
| 3.2 | Multiple sections and their wording was updated to align them to PA-DSS 3.2 | BTH | 13 NOV 17 |
| 3.3 | Modified section 9.0 Maintaining A | BTH | 23 JAN 18 |

| | | | |
|---|---|---|---|
| | Vulnerability Management Program and Section 10.0 Secure Remote Updates in alignment with PA-DSS 3.2 | | |
| 3.4 | Added Windows 10 to supported operating systems | BTH | 21 AUG 2019 |
| | | | |

# Travstar1  v10.01.02-XXXX_XXX
# 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  v10.01.02-XXXX_XXX in a PCI-DSS compliant retail environment. This guide will be updated at least annually to incorporate changes in the Travstar1 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, Inc. 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 that process payment transactions necessarily handle sensitive authentication data. The Payment Card Industry, founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, has developed security standards for handling sensitive authentication data 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 sensitive authentication data.

### Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

### Protect Cardholder Data

3. Protect stored cardholder Data
4. Encrypt transmission of cardholder data across open, public networks

### Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

### Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
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 for all personnel

The remainder of this document describes the essential guidance for implementing Travstar1 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 System

The Travstar1 does not store PAN or sensitive authentication data (i.e. CVV, CVV2 or PIN blocks) after authorization (PCI DSS 3.2.1, 3.2.2, 3.2.3). 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 masked or truncated 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 and thus PA-DSS req. 11.1.x does not apply. 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.

Travstar1 is not web based and does not require the use of a web server or storage of cardholder data on a web server.

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

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.

## 3.1 Travstar1 ® v10.01.02- XXXX_XXX Versioning Methodology

Fiscal Systems, Inc. defines the versioning methodology for the Travstar1, versioning elements are separated by a literal period, XX.XX.XX_XXXX-XX, as follows:

1st digit (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 PA-DSS.

2nd digit (Numeric) - This is the minor version number and would represent a minor enhancement to the application. This can include low impact PA-DSS changes but does not impact security.

3rd digit (Alpha Numeric) - This is the patch version number. When this is incremented, the release could involve defect patches. This digit would represent an internal non-compliance related change and is not intended to be public facing.  PA-DSS or security impacting changes are not represented by this digit.

## 4.0 Installing or Upgrading to Travstar1 v 10.01.02- XXXX_XXX

Instructions for installing or upgrading the Travstar1 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, option 3. Electronic format document viewing requires Adobe Acrobat reader.

Travstar1 has never stored SAD and thus no actions are required to meet PA-DSS req. 1.1.4.

The PAN is displayed truncated (first six and last four digits) by default in all instances, and thus not actions are required to meet PA-DSS req. 2.2.

## 4.1 REQUIRED PROTOCOLS, SERVICES, AND COMPONENTS

### Travstar1 Requires the following Ports / Services to function properly:

**Port:** 3555-3585 TCP Source**:** POS Destination**:** Site controller
**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

All other 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 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 Administrator 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.

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 1.0.2
Visual C++ 2008 Sp2

There is not dependent hardware. There is not dependent software, other than the OSs listed on section 13.0 OPERATING SYSTEM INFORMATION.

## 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. 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. These passwords must be managed at the operating system level. PCI-DSS requirement 8 covers these requirements. Each location is responsible for maintaining their own unique passwords. Travstar1 does not maintain these. Examples of default administrator accounts include "administrator" (Windows) and "root" (SuSE Linux).

PCI DSS 8.2.3 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 (PCI DSS 8.2.4)
- New passwords can not be the same as the last 4 passwords (PCI DSS 8.2.5)
- If an incorrect password is provided 6 times the account should be locked out (PCI DSS 8.1.6)
- Account lock out duration should be at least 30 minutes or until an administrator resets it (PCI DSS 8.1.7)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (PCI DSS 8.1.8)

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. (PCI DSS 8.1.1)

## 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 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

## 7.0 REMOTE NETWORK ACCESS

To comply with PCI DSS requirements, you must implement multi-factor authentication for remote access granted to the network for employees, administrators and third parties. TravsStar1 System does not directly facilitate any type of remote access that originates from outside the customer environment.

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

Travstar1 does not facilitate non-console administrative access. However, if you use remote access to perform non-console administrative access, you must use SSH, VPN or TLS encryption and the above security features to comply with PCI DSS requirements.

## 8.0 WIRELESS NETWORKING

Travstar1 is not developed for use with wireless technology and thus requirements PA-DSS 6.1 and 6.2 does not apply. 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.

## 9.0 MAINTAINING A VULNERABILITY MANAGEMENT PROGRAM

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 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 operating system be maintained automatically by using an automatic update service to download security patches daily. Refer to section 13.0 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 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, Fiscal Systems, Inc. will respond quickly to test and install available patches within 30 days on behalf of customers.

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 authentication 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 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

## 10.0 Secure Remote Updates

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. Notifications for new patches and updates are made via email.

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.

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 DSS 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)

- 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 AUDITING AND CENTRALIZED LOGGING

### Names and locations of POS System application logs:

Travstar1 by default will store logs in the files listed below, these logs are enable by default after the installation process and automatically configured to meet PCI DSS and thus not actions are required by the customer.

These locations are the only accessible area in which partial PAN data is available. All PAN data is truncated (First six and last four digits of the PAN) and defined as unreadable. There are no additional actions needed on the users' side to render this PAN data unreadable. Truncated PAN data is also available on customer receipts but is also defined as unreadable.

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)

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. Linux Payment Terminal (LPT)
   The log is named lptlog.dat and is located in /home/LPT.

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.

### CENTRALIZED LOGGING:

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 addressed at the beginning on this section.

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

## 12.0 System Troubleshooting

When troubleshooting cardholder problems, 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.

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 the PCI Data Security Standard requirements for the security of such transmissions.

The POS System does not store any sensitive authentication data or has a facility to email sensitive authentication data as part of the troubleshooting process.

## 13.0 Operating System Information

The current version of the Travstar1 application v10.01.02-XXXX_XXX validated under PA-DSS 3.2 supports the following operating systems:

| | |
|---|---|
| POS | Windows POS Ready 7 SP1, Windows 10 Enterprise LTSC |
| LPT | SUSE Linux Enterprise Server 11.4 |
| SC | SUSE Linux Enterprise Server 11.4 |
| CCL | SUSE Linux Enterprise Server 11.4 |

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.

## 14.0 Encryption Keys

The POS system automatically manages the encryption keys used to secure sensitive authentication data and PAN data during the preauthorization phase using AES-256 bit, not actions from the customer are required to meet PA-DSS 2.3, 2.5.x and 2.6. No sensitive authentication data is stored after a transaction is complete. The lifecycle of

encryption keys are controlled by two environmental variables in the CCL application environ.dat file.

KEY_ROTATION: This environment variable controls how often PCI encryption keys are rotated (changed), in minutes. See also KEY_DELETION. Acceptable values are any integer greater than zero and less than KEY_DELETION value. The default value is 43200 (30 days).

KEY_DELETION This environment variable controls how long the encryption keys are stored, in minutes. After this time period expires (counting from the time when the encryption key was created), data encrypted using that key can no longer be decrypted by the POS system. Acceptable values are any integer greater than zero and also greater than KEY_ROTATION. The default value is 129600 (90 days).

If it is necessary to manually force a reset of the POS system encryption keys:

1. Set the CCL environ.dat variables to:
   KEY_ROTATION 1
   KEY_DELETION 2
2. Exit all POS terminals
3. Run an “exit2” on the CCL
4. Start a POS terminal and log in
5. Exit POS
6. Change the CCL environ.dat variables back to their original values
   Default value for KEY_ROTATION 43200
   Default value for KEY_DELETION 129600
7. Run another “exit2” on the CCL
8. Start all POS terminals

## 16.0 REFERENCE

Payment Card Industry (PCI) Data Security Standard v3.2

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

## 17.0 REFERENCE

## 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.