



OPW Fuel Management Systems  
Payment Application Data Security Standards (PA-DSS)  
Implementation Guide for Maintaining PCI Compliance  
on the FSC3000 Fuel Site Controller

PA-DSS Implementation Guide  
Document Version 1.2  
March 2010

Table of Contents:

Application .....	1
Overview.....	1
Document Use .....	1
PA-DSS vs. PCI DSS Compliance .....	2
Product Certification Status.....	2
Acronyms & Terms .....	2
PCI DSS and PA-DSS Reference .....	3
Implementation of PA-DSS .....	4
Introduction .....	4
1. Do not retain full magnetic stripe, card validation codes or PIN block data .....	4
2. Protect stored cardholder data.....	4
3. Provide secure password features .....	5
4. Log application activity .....	5
5. Develop secure applications .....	5
6. Protect wireless transmissions .....	6
7. Test applications to address vulnerabilities .....	6
8. Facilitate secure network implementation .....	6
9. Cardholder data must never be stored on a server connected to the Internet .....	7
10. Facilitate secure remote software updates .....	7
11. Facilitate secure remote access to application .....	7
12. Encrypt sensitive traffic/data over public networks.....	7
13. Encrypt all non-console administrative access. ....	8
14. Maintain instructional documentation and training programs for customers, resellers and integrators.....	8
Merchant's requirements for maintaining PCI compliance.....	9
Creating and maintaining users.....	9
User logon and passwords.....	9
Third-Party Application Interfaces / Remote Access.....	9
OPW Device Connections.....	9
External USB Journal Key.....	10
Remote Access via Dial-in Modem .....	10
System Logging and Maintenance .....	10
Automatic print and clear of log data .....	10
Manual capture of log data .....	10
Returning System for Warranty or Repair.....	11
Additional requirements for securing sensitive data.....	11
Creating a Compliant Environment when Upgrading an Existing FSC3000 .....	11
FSC installed before Aug 1, 2008, and Does NOT Use the Ethernet Port for Remote Access .....	11
FSC installed before Aug 1, 2008, and USES the Ethernet Port for Remote Access.....	11
FSC installed after Aug 1, 2008, and USES (or will use) Ethernet Port for Remote Access	12
FSC3000 System Installation .....	13
Setup .....	13
Card Processing .....	13

“System Start” command.....	13
Privileged vs. Partial Access.....	13
Users .....	13
“Set Admin” command.....	13
User Options .....	14
Passwords.....	14
Login command and administrator access .....	14
Remote access login via Ethernet port.....	14
System Activation.....	15
Recommended Startup/Installation Process.....	15

## Application

This document supports the OPW Fuel Management System's Petro Vend Fuel Controls FSC3000 Fuel Site Controller running Multi-trucking Network Software with:

PA-DSS Compliance Version: 1.0

Card Record Feature Version: 1.09c or higher (regardless of model or system configuration).

*Note: Some configurations should not be used when Bankcard Payment Processing is in use. These configurations are mentioned and discussed within this document.*

## Overview

OPW Fuel Management Systems has redesigned setup/configuration control, user access and data access on the FSC3000 platform, in order to provide you a Visa U.S.A. PABP (Payment Application Best Practices)/PCI PA-DSS (Payment Application Data Security Standard) system that can be installed in a compliant manner. We have redeveloped the multi-trucking application to offer a product that now operates in accordance with PABP/PA-DSS guidelines. These guidelines are designed to assist software developers and application/equipment providers in deploying secure software platforms that provide merchants the control to comply with Visa's "Cardholder Information Security Program" (CISP). With the proper use, setup and maintenance of the FSC3000 as described within this document, OPW is working to help you provide a secure environment for the processing and safety of your customer's bankcard information and privacy.

The FSC3000 is designed to be flexible and support the vast range of features requested by our customers. OPW has attempted to incorporate the required changes without directly affecting the daily operations of those customers not processing bankcards and therefore not required to comply with the requirements. However some of the procedures and control normally used to support the system have been changed. Therefore, whether you process bankcards or not, please take the time to read this document for a clear understanding of the changes employed and the steps you must follow to operate and work with the redesigned multi-trucking network software.

## Document Use

This PA-DSS Implementation Guide contains information for proper use of the multi-trucking network application. OPW Fuel Management Systems does not possess the authority to state that a merchant may be deemed "PCI Compliant" if information contained within this document is followed. Each merchant is responsible for creating a PCI-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the multi-trucking application in a manner that will support a merchant's PCI PA-DSS compliance efforts.

***Note: Both the System Installer and the Controlling Merchant must read this document.***

## PA-DSS vs. PCI DSS Compliance

As an equipment vendor, our responsibility is to develop a software application to be PABP/PA-DSS Compliant. This applies to all software vendors who develop payment applications that store, process or transmits cardholder data as part of authorization of settlement. The software application itself is subject to an independent third-party audit that generates a certification report, which is then certified by the PCI Security Council. We have performed an audit and certification compliance review with an independent auditing firm to ensure our application/equipment conforms to industry best practices when handling, managing and storing payment-related information.

PCI DSS Compliance ultimately falls on you, the merchant. It's your responsibility to work with your hosting provider, use PCI-compliant server architecture with proper hardware and software configurations and access-control procedures.

Following the procedures and steps defined within this document will help you on your way to incorporate PCI DSS Compliance. It is up to you as the merchant to continue to implement and live by the rules defined to ensure you meet the requirements defined by the Payment Card Industry (PCI) Data Security Standards (DSS). The security requirements defined in the DSS apply to all members, merchants and service providers that store, process or transmit cardholder data. These requirements also apply to all system components within the payment-application environment, which is defined as any network device or application included in or connected to a network segment where cardholder data is stored, processed or transmitted.

## Product Certification Status

The FSC3000 multi-trucking network software was evaluated by:  
PSC (Payments: Security: Compliance) San Jose, CA, an independent auditing corporation.

Validated PA-DSS v1.2 complaint by the PCI Security Standards Council, Dec. 2008  
Reference #: 09-05.00508.001, revalidated: Jan 7, 2010 (ref#: 09-05.00508.001.aaa)

## Acronyms & Terms

The follow is a list of acronyms and terms used within this document:

**PA-DSS:** PABP (Visa's Payment Application Best Practices)/PA-DSS (Payment Application Data Security Standard)

**OPW:** OPW Fuel Management Systems

**FSC:** FSC3000 Fuel Site Controller (and the multi-trucking software operating within).

**Distributor:** The equipment reseller and integrator. A qualified individual certified by OPW for the installation of the FSC3000.

**Merchant:** The owner/operator of the fueling location at which the FSC is installed.

**User:** A (case sensitive) name that has been added to the FSC, by the merchant, to allow system logon access. Users have full command line access of the system, except for network setup that is now Admin control only.

**We:** Throughout the sections below the term "We" is used. This term always refers to the OPW development team that created and designed the software application.

**PAN:** Personal Account Number (number embossed on bankcard)

**SIMM:** Single In-line Memory Module. The memory card inside the FSC3000 used to store the payment application and transaction information.

### **PCI DSS and PA-DSS Reference**

As the merchant (and/or the equipment reseller/integrator), you should download the “Payment Card Industry, Data Security Standard: Requirements and Security Assessment Procedures” to further understand your requirements for implementing and maintaining a compliant environment under which to operate.

To learn more about PCI compliance standards visit: <https://www.pcisecuritystandards.org/>

## Implementation of PA-DSS

### Introduction

The OPW Fuel Management Systems FSC3000 multi-trucking application has been developed and tested according to the Visa U.S.A Card Information Security Program (CISP) Payment Application Best Practices and the PCI PA-DSS Documentation. This section covers the different sections of these documents and the actions OPW has taken to implement the requirements of each.

#### 1. Do not retain full magnetic stripe, card validation codes or PIN block data

It is the responsibility of the application developer to ensure prohibited magnetic-stripe data is not stored or retained anywhere within the system. This implementation is designed to meet the requirements of PA-DSS from 1.1 through 1.1.5 which in turn meets your requirements of PCI DSS 3.2 through 3.2.3 where:

- 3.2 - States sensitive authentication data should not be stored after authorization.
- 3.2.1 – Do not store full contents of any track/magnetic-stripe data.
- 3.2.2 – Do not store card-verification code or the 3- or 4-digit number printed on the front or back of a payment card.
- 3.2.3 – Do not store the Personal Identification Number (PIN).

We developed the FSC to retain magnetic-stripe data in active memory until the authorization process for fueling is complete. At that time, the memory locations used to retain that data are wiped and ready for the next card presented.

**Note:** Currently the FSC does not prompt for card validation or PIN block data. No sensitive authentication data is written to transaction storage memory.

#### 2. Protect stored cardholder data

It is the responsibility of the application developer to mask any displayed cardholder data. Storing none of the cardholder's sensitive data, including the PAN, supports this requirement. Being an embedded system, the storage of transaction data and cardholder information is not stored in a typical database but within formatted battery-backed non-volatile memory. Although this memory is not even accessible from within the system, we have chosen to support this requirement in the following manner: Upon completion of capturing the final sales data with the network host, we wipe the cardholder's expiration data from the transaction record and clear the account number portion of the PAN, except for the six-digit ISO and the last four digits. Under this process the full PAN is not even available for the Administrator to reference. This implementation allows us to comply with PCI-DSS requirements 3.3 through 3.6, which state:

- 3.3 – Mask PAN when displayed (we only show last 4 or first 6 and last 4 digits).
- 3.4 – Render PAN unreadable anywhere it is stored/displayed (we wipe Account portion of PAN).
- 3.5 and 3.6 – Protect cryptographic keys and document key management (by wiping Account portion of PAN we don't use encryption to protect data).

PCI-DSS 3.1 states that cardholder data be purged after a customer-defined retention period. Based on how memory is used within the FSC, previous cardholder is purged (overwritten) each time the transaction buffer is cleared and new cards are used in the system. To ensure this process occurs in a timely manner to meet the defined retention period, the transaction buffer size should be defined to ensure that it is either cleared regularly or automatically overwritten by enabling the transaction buffer auto-wrap feature.

### 3. Provide secure password features

It is the responsibility of the application developer to ensure unique user names and complex passwords for all administrative access and access to cardholder data. We control this requirement by ensuring default factory passwords are changed before installation is complete. Due to the nature of our system and the process required to install and configure the FSC, we have designed the system to be shipped with no defined users and an inactive administrator login. Once installed and configured the administrator login (entered as: "Admin") must be activated and a password created. The factory default passwords used to access the system (even at its lowest level) must also be changed.

We recommend the following when creating users and passwords, and accessing the system:

- As stated above, forcing you to change all factory-default passwords, creating an administrator password and defining users with case-sensitive names helps us control PCI DSS requirement 8.1 and 8.2.
- For further protection of the administrator password we suggest:
  - Don't use the "Admin" login as the normal way of accessing the FSC.
  - Consider creating an "Admin" password set to max entry length of 15 and then not using it to access the FSC except for network setup and the management of users and passwords.
- Create and maintain PCI DSS-compliant authentication access by following PCI DSS requirements 8.5.8 through 8.5.15. We have helped here by strictly enforcing requirements: 8.5.10, 8.5.11, 8.5.13, 8.5.14 and 8.5.15.

**Important:** Attempting to change or manipulate "out of the box" payment software installation settings that control limits, lengths or criteria of how user names and secure authentication (passwords) are accepted will result in non-compliance with PCI DSS.

*For more information about users and passwords see: "Merchant's requirements for maintaining PCI compliance" and "FSC3000 System Installation" sections below.*

### 4. Log application activity

It is the responsibility of the application developer to log all user access to cardholder data. As described in topics 1 and 2 above cardholder data is not saved and therefore user access to cardholder-sensitive data is not possible. In an effort to conform to this requirement we chose to create a logging mechanism that not only records which users view transaction information, but any changes to system access and configuration. This logged data is stored on the system in flash on FSC3000 SIMM so data is retained even if a system Cold Start is performed. Under terminal/console access only the Administrator can clear log data.

We have developed the log to meet the PCI DSS requirements defined in sections 10.1 through 10.2.7. In addition, the information logging meets the requirements defined in sections 10.3.1 through 10.3.6 by logging: username, action taken, date and time and the access point used.

*For more information about managing the system log information see: "Merchant's requirements for maintaining PCI compliance" section below.*

**Important:** Disabling the system log process in any way will result in non-compliance with PCI-DSS.

### 5. Develop secure applications

It is the responsibility of OPW and all of its designers to provide a product and payment application that is developed in accordance to PCI DSS requirements. These requirements are specific to the design, control and production and testing of the product and its software. They require us to: maintain software and hardware revision control; develop applications based on industry best practices and incorporate information security throughout the development life cycle; perform application code reviews and walkthroughs to identify vulnerabilities; use separate development and test environments with the separation of responsibilities; not ship applications

with test accounts for debugging information used during development and testing; provide secure update and back-out procedures; and PCI-specific testing to ensure approved implementations are maintained as updates and new releases occur.

The FSC300 multi-trucking network application has been developed in accordance with these procedures and we have put in place specific controls to ensure these practices are maintained for future development. These procedures and policies ensure our application meets the PCI DSS standards described in sections: 6.2, 6.4 and 6.5.

## 6. Protect wireless transmissions

It is the responsibility of the implementer and the Merchant to ensure that any wireless connections provided as part of the interface to the payment environment are secured according to PCI DSS requirements. The FSC3000 under normal installation conditions does not use any wireless connections as part of the interface that transmits cardholder-sensitive data.

The Merchant (*including Distributor Technicians*) **MUST** not install wireless Petro-Net modems between the FSC and Terminal Card Readers (such as the C/OPT or FIT500). Doing so would violate PCI DSS requirements and make your system non-compliant!

In addition, the Merchant should not use/install any wireless devices connected to the FSC. If you as the Merchant install a wireless device it is your responsibility to ensure the wireless connection is not available for access outside of a secure firewall. If you must use wireless technology connected to the FSC, you must ensure it is implemented in accordance with the following PCI Data Security Standards:

- 1.2.3 – Install perimeter firewalls between any wireless networks and the cardholder data environment.
- 2.1.1 – For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults such as keys and passwords.
- 4.1.1 – Ensure wireless networks transmitting cardholder data use industry best practices (for example: IEEE 802.11i) to implement strong encryption for authentication and transmission. *For new installations it is prohibited to use **implement WEP**.*

**Important:** OPW accepts no responsibility for the installation of a wireless device for the purpose of remote access to the FSC. Failing to install payment applications in wireless environments according to PCI DSS requirements 1.2.3, 2.1.1 and 4.1.1 will result in non-compliance with PCIDSS.

**Important:** *Internal Bluetooth and cellular modems will NOT be allowed to operate within the FSC3000 when a network approved for the processing of bankcards is enabled. If a wireless device is configured or detected by the system, the software will disable the internal socket's serial port from use. If the software determines the internal device is configured incorrectly regardless of installed networks, the port will also be disabled from use.*

## 7. Test applications to address vulnerabilities

It is the responsibility of the application developer to ensure that payment applications are tested for security vulnerabilities according to PA-DSS requirements 6.2, while ensuring updates and patches are delivered in a secure manner. OPW performs internal regression testing before every software release to ensure PA-DSS requirements are always maintained within the system. Updates to the payment application are only available to Certified Trained Distributor Technicians via a secure login at OPW Fuel Management Systems Technician-only Web page or directly from the OPW Technical Support Group.

## 8. Facilitate secure network implementation

It is the responsibility of the application developer to ensure remote access is performed securely and to ensure non-console access uses strong encryption and does not interfere with a secure

network environment. All access points to the FSC, including its TCP/IP Ethernet port, interact and limit access to a terminal console interface. When making remote access connections using the FSC TCP/IP port, the FSC must be on a private LAN behind a secure firewall. **You Must Not Connect the FSC to an open Internet connection.** To further protect the FSC when connected to a network via the TCP/IP port, Administrator access is not allowed. The administrator MUST always login via the direct connect terminal port or by using the dial-in modem.

When installing the FSC in a network environment it is your responsibility as the merchant to review and strictly follow PCI DSS requirements:

- 1.1 through 1.4 that relate to the installation and maintenance of a network firewall.
- 4.1 and 4.2 we help you conform to these requirements by never sending or displaying sensitive cardholder data out any FSC access point.

#### 9. Cardholder data must never be stored on a server connected to the Internet

Although the FSC never transmits cardholder-sensitive data outside of the controller, it is the merchant's responsibility to ensure that whatever server (or PC) is used to poll transaction data is not directly connected or exposed to the Internet.

Refer to PCI DSS requirement 1.3.2 for more information on limiting access to the DMZ.

#### 10. Facilitate secure remote software updates

It is the responsibility of OPW to provide secure software update procedures under PCI DSS. As described in number 7 above updates are available from a secure distributors' section of our Web site. Only certified OPW Distributor Technicians or OPW Technical Service Group technicians should perform software updates to the FSC. To further ensure secure updates, OPW recommends that application updates only be performed using the direct-connect serial port or the dial-in modem interface.

For more information regarding secure remote updates, refer to the PCI DSS requirement 1 for information about installing and maintaining firewall configuration to protect data along with section 12.3.9 for activation of remote access for vendors only when needed.

*Refer to "FSC3000 System Installation" below for more information about creating a "Time Limited Login" for Vendor and Distributor access.*

#### 11. Facilitate secure remote access to application

All remote access points to the FSC, whether from a modem or the Ethernet port, interact as a terminal console interface connection requiring a "Remote Connect" password and then a "Partial Access" password. Under this connection a minimal command set is allowed providing the ability to poll transaction data (containing NO bankcard or cardholder-sensitive data) and manage the internal proprietary card file. Without entering an additional login sequence (requiring a case-sensitive username and password) further access rights are not available (*See: "Merchant's requirements for maintaining PCI compliance" and "FSC3000 System Installation" sections for more information about user names and passwords*).

It is recommended that a dial-in modem be physically connected to a phone line only when the need for remote access is required for the purpose of polling or system management.

**Important:** For additional information on how to facilitate secure remote access, you must reference PCI DSS requirements 8.1 through 8.4 and 8.5.8 through 8.5.15.

#### 12. Encrypt sensitive traffic/data over public networks

Because the FSC does not retain any sensitive bankcard or cardholder data, it cannot transmit this information over a public network. The only cardholder data ever transmitted from the FSC is the 6-digit ISO (user specific) and the last 4 digits of the PAN. To further ensure the protection of

sensitive data it is the merchant's responsibility to ensure the FSC is never connected to a public network (*For more information regarding the transmission of the 6-digit ISO numbers refer to the "Users Options" information under the "FSC3000 System Installation" section of this guide*).

Refer to PCI DSS requirements 4.1 and 4.2 for additional information regarding the encryption of transmissions across open public networks.

**13. Encrypt all non-console administrative access.**

Although the FSC allows remote access via the Ethernet port, the interface provided under this connection type is designed to operate as a terminal console interface. However, in order to maintain PCI compliance in regards to this topic and PCI DSS requirement 2.3, administrator access is not allowed using the Ethernet port. (*See: "FSC3000 System Installation" section for more information about using ether-net port for remote access*).

**14. Maintain instructional documentation and training programs for customers, resellers and integrators**

This Implementation Guide is designed to provide you with the instructional documentation required for maintaining a PCI-compliant environment using the FSC3000. Our resellers/distributors are trained in the installation and implementation of the FSC3000 and provided PCI compliance information in the form of this guide.

As the merchant you should question your distributor to determine if they have been trained by OPW and explained the requirements defined within the guide, before allowing them to install the FSC3000 in your facility.

## Merchant's requirements for maintaining PCI compliance

This section describes the steps and responsibilities required by the merchant in order to maintain PCI compliance with the FSC3000.

### Creating and maintaining users

Users and unique passwords should be created before the FSC is activated for use. *For more information on creating users, see the "FSC3000 System Installation" section below.*

Up to 5 users with case-sensitive names can be defined for access to the system. You should not allow more than one user to access the system with the same username and password (usually referred to as group access). User names should always be deleted from the system if that person leaves your company or changes to a position that does not require access to the FSC.

*Note: User names on the FSC are a maximum length of 10 characters. Because user names are case-sensitive, creating them with a combination of caps and lower-case characters adds another level of login security.*

### User logon and passwords

Users logging onto the system who have forgotten their passwords, will be locked out of the system for 30 minutes after six bad password attempts. To allow access within that time frame the administrator must logon and reset the user's password.

To maintain continued compliance, you must manage passwords using these rules:

1. Change user passwords, including remote and partial-access passwords, after 90 days.
2. The new password cannot be the same as any of the last 4 passwords for that user.
3. Passwords should be unique for each user.

Because passwords cannot be retrieved from the system, it is IMPORTANT that you record and store the administrator password in a secure location. If you lose or forget the administrator password, you must COLD START the FSC in order to reset the administrator password.

Note: Sessions idle for more than 15 minutes are automatically logged off.

### Third-Party Application Interfaces / Remote Access

OPW cannot control how third-party applications manage passwords or try to interact with the system. In order to further protect the payment system and cardholder-sensitive data, OPW has reduced the command set available to these applications. With the PA-DSS compliant release, third-party applications will only be able to poll transaction data that contains no bankcard or cardholder-sensitive data (*Only the last four digits of a cardholder's PAN can ever be polled by these third-party applications*) and perform card-management functions against the internal proprietary card file. Along with the limited command set, these applications are now required to access the system at the Partial Access (or Privileged) prompt. The "SH TRANS CF", Card Update, Card Restore and Card Backup commands are no longer available in non-Privileged mode.

OPW recommends you contact the vendor of any third-party application you may be using and request updates to provide secure password management or removal of password storage all together.

### OPW Device Connections

When installing the FSC and its peripherals (such as: FITs, C/OPTs, FIT500s, PCMs or even UPCs), wireless modems should not be used as a connection solution for Petro-Net. Direct wiring must be used

to establish a connection between the FSC and its associated devices to ensure a PCI-compliant installation. Internal Bluetooth and cellular modems cannot be installed in the FSC, only a standard dial-in modem can be used for remote connections.

**Important:** *Internal Bluetooth and cellular modems will NOT be allowed to operate within the FSC3000 when a network approved for the processing of bankcards is enabled. If a wireless device is configured or detected by the system, the software will disable the internal socket's serial port from use. If the software determines the internal device is configured incorrectly regardless of installed networks, the port will also be disabled from use.*

### **External USB Journal Key**

When a journal printer is not desirable due to the location of the installation or the environment, an external USB key can be used in place of the journal printer. The FSC will create a transaction history log file on the USB key in the same data format that is provided to the third-party polling applications, as described above.

Where the transaction data contains no bankcard or cardholder sensitive data, *only the last four-digits of a cardholder's PAN will ever be written to the file created on an external USB journal key.*

### **Remote Access via Dial-in Modem**

In order to maintain a higher level of security with remote access, it is recommended that dial-in modems be physically connected to a phone line only when the need for remote access is required for the purpose of polling or system management.

## **System Logging and Maintenance**

OPW has implemented an always-on system-logging process. This logging mechanism is designed to track events such as: user creation, password changes, logins, system resets and cold starts, users who view transaction data, and more.

Under the current implementation of this logging mechanism the data is stored in one of the flash banks located on the FSC SIMM card. Because the available space allocated to logging is fixed, the available log space could fill and therefore stop the logging the process from continuing (*current tests indicate about 2,000 to 2,100 entries can be made*). PCI compliance states that the merchant must retain a minimum of one year of log data. In order to help you meet this requirement, OPW has implemented an automatic log print process to the journal printer. If you're operating without an active journal printer, it is your responsibility as the merchant to capture log data manually and retain it for one year.

### **Automatic print and clear of log data**

Under the journal printer setup (SET JOURNAL) you will be prompted to automatically print log data on the first day of each month. Answering, "Yes" to this prompt will cause the system to automatically print the current log data on the first day of every month following the printing of midnight totals. Once printed, the FSC will automatically clear the log file and starts again to continuously log system activity.

### **Manual capture of log data**

If you do not have a journal printer installed or prefer not to auto-print the log you must manually capture and store log data to maintain your PCI compliance. To manually capture log data use the following procedure:

1. Connect to the FSC using a terminal application that provides the ability to capture text. This includes applications such as: HyperTerminal, ARTWare or Phoenix.
2. Log into the FSC using the "Admin" login ("login Admin")
3. From within the terminal application, enable text capture.
  - a. Do not overwrite an existing capture file that is not more than one year old.
4. From the command prompt: "Admin>" issue the command "SHOW LOG"

5. After the log data has been completely displayed, turn off the terminal's text-capture feature saving the capture file in a save location that be can accessed for at least one year.
6. From the command prompt: "Admin>" issue the "SET ADMIN" command and select the "Clear Activity Log" option. This will clear the flash blank and then log an entry indicating when the clear process occurred.
7. Press "Enter" to exit the "Administrator Menu."

### **Returning System for Warranty or Repair**

As the merchant you are responsible to ensure that no sensitive bankcard or cardholder data is allowed to leave your facility. Therefore, if you need to return the FSC to OPW or your local distributor and bankcard transactions have been processed, the transaction storage memory must be wiped.

Follow these steps to ensure transaction memory is cleared.

1. Disconnect power to the FSC and remove the cover.
2. Locate the battery on the SIMM card and place a piece of paper between the battery and its hold clip.
3. Allow this paper to remain in position for minimum of four minutes. This will allow the battery's backed-up memory to decay, removing any sensitive data from the system.
4. Remove the paper and reattached FSC cover (or allow to remain to conserve battery life).
5. The FSC is now safe to release to OPW or your distributor.

### **Additional requirements for securing sensitive data**

This section covers additional requirements defined by the PCI Security Standards Council not already discussed elsewhere in this document. This organization has further enhanced the requirements and guidelines initially defined by VISA U.S. in the PABP. The new guidelines are referred to as: "Payment Application Data Security Standards" or "PA-DSS."

The above procedure "*Returning System for Repair or Warranty*" can also be used before upgrading your site from previous versions of FSC software not certified as PCI-complaint. This provides compliance for the PA-DSS requirement 1.1.4: "Delete sensitive authentication data stored by previous application versions"

### **Creating a Compliant Environment when Upgrading an Existing FSC3000**

If you currently own a FSC3000 Fuel Site Controller and you are preparing to upgrade to a PCI-certified compliant version of software several steps may be required to ensure the existing FSC is used in a manner that meets compliance. Reference the topics below that apply to you and follow the define steps.

**Note:** If this is a new site installation you can skip this section.

#### **FSC installed before Aug 1, 2008, and Does NOT Use the Ethernet Port for Remote Access**

If you installed your FSC prior to this date then you have FSC board revision "B." You can upgrade your application software and continue using the FSC as you do today. However, if you ever connect an Ethernet cable to provide TCP/IP access to the system, you MUST then follow the next topic.

#### **FSC installed before Aug 1, 2008, and USES the Ethernet Port for Remote Access**

If you installed your FSC prior to this date then you have FSC board revision "B." Using the Ethernet port on this version FSC, as it is today, does not allow you to operate in a compliant environment. You must therefore choose one of the processes below to ensure compliance.

**Note:** If you need assistance with any of the processes defined here, please contact the OPW Technical Service Group for support to ensure the process is completed successfully.

Process 1: Return the FSC and upgrade to a new controller directly from OPW Fuel Management Systems.

Process 2: Disable Ethernet Web interface. This process should only be used if you don't expect to connect any external devices to the FSC requiring the possible change to your system's connection point baud rates (*if you expect to add external devices follow process 1*):

1. Access the Web interface (available from any browser) for the Ethernet controller. This can be done by entering the IP address of the FSC into the address bar of your browser or by selecting the "Open Web interface" option using the Digi Device Discovery tool (*provided on the ARTWare installation CD*).
  - a. If a login screen is presented the username is "root" and the password is: "dbps"
2. Under the "Configuration" menu on the left, click on the "Network" link.
3. From the Network Configuration screen (at the bottom) select the "Network Services Settings" link.
4. Under this section disable (or uncheck) the following options: a) "Enable Telnet Server" b) "Enable Web Server" and "Enable Remote Login."
  - a. Click the "Apply" button. Your browser should now display an error indicating the page cannot be found. You are now ready to operate in a compliant environment.

#### **FSC installed after Aug 1, 2008, and USES (or will use) Ethernet Port for Remote Access**

Before continuing with this process, remove the cover of the FSC and determine the board revision you have. The revision letter of the board can be found on the front edge directly beneath the right side of the display, to the left of a white square. If the board revision is "B" you can follow process 1 or 2 above. If the board revision is "C" follow the steps below. When complete and the software has been upgraded you will be to switch port baud rates as needed.

1. Access the Web interface (available from any browser) for the Ethernet controller. This can be done by entering the IP address of the FSC into the address bar of your browser or selecting the "Open Web interface" option using the Digi Device Discovery tool (*provided on the ARTWare installation CD*).
  - a. If a login screen is presented the username is "root" and the password is: "dbps"  
OR
  - b. If your browser displays an error indicating the page cannot be found, then your system was configured as needed from the factory and you can proceed with the software upgrade. Skip the remaining steps.
2. Under "Configuration" menu on the left, click on the "Serial Ports" link. When the "Serial Port Configuration" screen is displayed click the "Port 1" link.
3. Scroll to the bottom of the page and click on the "Advanced Serial Settings" link.
4. Under the section "Serial Settings" locate the checkbox option "Enable RCI over Serial (DSR)" and check the checkbox (*You Must See This Box Checked!*). Scroll down and click the "Apply" button.
  - a. After the screen refreshes, ensure a message at the top reads: "Changes have been saved successfully." Double check that this is checked before proceeding to step 5.
5. Using ARTWare, update the FSC to the latest version of PCI-complaint software.
6. After cold start/reset you should see this message displayed at the CAP port; "LAN Device Configured." If not, repeat step 1 above. You should see the condition under 1.b.
  - a. If NOT please contact OPW Tech Support for further troubleshooting.

## FSC3000 System Installation

### Setup

Setup of the FSC hasn't changed, but availability of the command-line interface has been altered to reduce user access once the system has been activated ("Started") for the processing of cards. These changes and how they affect system use are explained throughout this section (*FSC3000 System Installation*).

*Note: Distributors unfamiliar with the new setup and configuration of this software version should contact OPW's Technical Service Group for assistance.*

### Card Processing

The FSC will not process any cards without the system being activated for use. Your distributor will be able to install and configure the system as needed, but the processing of any cards (*including PCF-defined and Private Fleet*) is not allowed until the factory default passwords (*Remote Access, Partial Access (previously known as "Privileged") and the Administrator password (new for PA-DSS compliance)*) are changed and the "System Start" command is issued.

### "System Start" command

Requirements of PA-DSS compliance forced the creation of new commands designed to strengthen security and user access to the system. The "System Start" command, which is only available after the factory default passwords have been changed, causes two main actions to occur. One activates the system to allow the processing of cards and the other changes the availability of system configuration commands. Once the system has been "Started" all command-line setup is disabled, unless logged in as one of five merchant-definable users or the administrator. Once started, the system cannot be stopped. All configuration commands (including some "Show") are available only when logged onto the system.

### Privileged vs. Partial Access

Historically, OPW FSCs allowed for two levels of access: "Show" and "Privileged." Privileged access allowed for complete control of the system while "Show" only allowed a user to see information but never alter it. The "Show" access mode has been eliminated completely and "Privileged" mode is now dependent on system activation. Before system activation "Privileged" mode operates as it always has, but once activated this access level changes to "Partial Access" mode. Partial access mode provides the ability to see system settings with limited ability to "Set" daily system functions. Some of these daily commands include: "Set Fueltype" for pricing changes, "Set Pump On" for manual activation of a pump and "Install Pump X" so individual pumps can be placed back in service due to activation of the Pump Sentry feature.

*Note: The "Show Trans" command is only available to logged-in users.*

### Users

To provide a stronger level of security, individual user logon access has been added to further support PCI compliance. You are able to create up to five individual user names for system login. Each user name is case-sensitive and can be assigned its own password. In addition to these five users, a factory-defined username of "Admin" has also been added to the system. This administrative user has been specifically designed for the purpose of managing users and password and clearing the system activity log, it cannot be deleted. When defining users OPW recommends the creation of a user called "Tech" with a unique password that can be used to provide access to your distributor's technician or OPW's Technical Service Group. This password can then be assigned as needed to operate for a limited number of days (*See below for more information about creating users*).

### "Set Admin" command

This command allows you to define up five individual users of the system. They can be created and deleted or have their passwords changed whenever the system administrator desires. This command

is also used to initially change the factory default passwords for the Remote and Privileged (Partial Access) logins, along with managing the administrator password. It is available for use under the Privileged login until the administrative password is defined. Once set, this command is ONLY available under the “Admin” login. This now provides the administrator exclusive access for the management of system users.

### User Options

When creating users, two configurable options are available; one defines how card numbers are displayed for bankcards when viewing transactions and the other is a “Limited Logon” option that allows you to define a limited number of days for which logon can occur. The card number option allows you to say whether a user can view just the last four digits of a card number or the 6-digit ISO along with the last four digits (displayed as: 123456xxxxxx4321). The limited logon option is useful for a “Tech” login (*as recommended above*), or someone who needs brief access to test or troubleshoot the system. Each time the password for a “Limited Logon” user is set, the administrator can define how many days (up to 15) this user is allowed to access the system. Once the number of defined days is passed, that user’s logon is no longer valid until the password is reset.

### Passwords

Coupled with the addition of individual user access, password creation and management has been modified to: 1. Ensure all passwords are uniquely encrypted on each FSC using a SHA1 hashing algorithm, 2. Remove the ability to decode a password by the OPW Tech Service Group, 3. Disable system functionality until factory default passwords have been changed. In the case of the FSC, this means that no cards can be processed without changing the factory default values and 4. Require strong password-creation rules. OPW has instituted the follow rules for password creation:

- Must be a minimum of 8 characters in length, with a max length of 15.
- Each password must contain at least:
  - 1 capital (or upper-case) letter
  - 1 lower-case letter
  - 1 numeric digit
- Special characters (those available on a standard keyboard) are allowed but not required.

**Important:** Whenever the administrator password is changed, you must record this information and store it in a safe place. If you lose or forget the administrator password you must “Cold Start” the system to regain access to the “Set Admin” command.

### Login command and administrator access

Once users are defined, they must login using the “Login <username>” command. As stated above user names are case-sensitive. If when created, the administrator entered “Tech” as the username, an entry of “login tech” will not be valid.

Once the administrator password is set the “login Admin” command must used be to gain administrative access. This controlled access allows and is restricted to:

- “SET ADMIN” command, to manage users and clear system log.
- Use of the “SET NETWORK” and “SET FLEET” commands
- All available system configuration commands.
- Disabled access via the Ethernet port. *User must login using direct connect or dial-in modem.*

**Note:** If a user (including the “Admin”) enters an incorrect password five times in a row, that account will be suspended from use for 30 minutes.

### Remote access login via Ethernet port

As stated above, remote access is not allowed for the Administrator (“Admin”) using the Ethernet. If remote access is be used as the primary connection point, via the Ethernet port, it is important to ensure at least one additional user is created.

## System Activation

Once setup is complete, the factory-default passwords have been changed (using the “Set Admin” command) and the desired users have been created, issuing the “System Start” command will allow the processing of cards and the disabling of Privileged mode.

## Recommended Startup/Installation Process

Because of the PA-DSS changes made to the software, OPW recommends the following setup steps to ensure the simplest installation process of the FSC3000.

1. As explained above, login to “Privileged” mode and issue the “SET DATE” and “SET TIME” commands. Because the system log is active on cold start, the date and time should always be set first to ensure the correct timestamp is logged to all further commands.
2. Install and configure the system as needed to ensure terminals are configured and running. Pumps should be installed and operational (using the “SET PUMP ON” command to test pump installation). Network configuration information should be entered for each network enabled.
3. If attached, configure the office journal printer to automatically print the system log on the first of every month.
4. Issue the “Set Admin” command. Change the factory default passwords for Remote and Partial access. Create an administrator password (be sure to record and store the administrator password).
5. Create additional users for access to the system.
6. Issue the “System Start” command. Cards can now be processed and fueling can occur.