PA-DSS Implementation Guide

for the AcuSport® V6 System Software

January 2015

AcuSport®
Retail Technology Group

940 Industrial Drive, Suite 107
Sauk Rapids, MN 56379
1-800-547-7120

Notices

940 Industrial Drive, Suite 107
Sauk Rapids, MN 56379
1-800-547-7120

General

No part of this document may be reproduced, distributed, performed, displayed, or used to prepare a derivative work without the prior and express written consent of AcuSport Corporation (“AcuSport”). The software described in this document is furnished under a license agreement and may be used only in accordance with the terms and conditions of the license agreement. Information in this document is subject to change without notice, and AcuSport assumes no responsibility for errors.

Trademarks and Credits

ACUSPORT, AXIS, AXIS Retail Management System (AXIS RMS), AXIS Data Center, AXIS Register, and AXIS E4473 are trademarks of AcuSport and shall not be used without the express written permission of AcuSport.

Other trademarks, such as QuickBooks, are not being used as a trademark herein and are the property of the respective owners.

Legal Counsel

This program, printed documentation, and documents should not be used as a substitute for professional advice in specific situations. The procedures, images, and examples in this document are for illustrative purposes only and may not be applicable in your setting due to differences in preference, settings, and/or state and local regulations.

The following notice is required by law:

AcuSport products and services are not a substitute for the advice of an Attorney.
You are encouraged to seek the advice of your own attorney concerning the use and legality of this program, documentation, and forms.

Publication Information

PA-DSS Implementation Guide for the AcuSport® V6 System Software
January 2015

Contents

Introduction

This guide provides details that define how to properly deploy the V6 6.0 application within an environment to help achieve PCI DSS compliance. Following the guidelines within this guide does **NOT** make the customer PCI DSS compliant, nor does it guarantee the customer network's security. It is the customer's responsibility to ensure that hardware and network systems are secure from internal as well as external threats. While this guide will go over the requirements the customer will need to follow for the implementation of V6 that will help achieve PCI DSS compliance, it is the customer's solely responsibility to ensure the proper implementation of the application.

AcuSport makes no claims on the security of the customer's network, nor of the level of PCI DSS compliance.

This guide is distributed to all internal AcuSport customer support staff and to all customers of the V6 application. Updates to this guide will be delivered to each customer's registered point of contact with a summary of changes discussing possible impacts to deployment or environment. These same updates are available through the AcuSport support site for registered customers. All AcuSport customer support staff are trained on any updates to the application and implementation guide prior to the release of the application. Should further explanation be required, customers may contact support at 800-547-7120.

V6 is a complete retail management system with a POS and IMS designed specifically for the firearms retail industry. The application supports Visual FoxPro application/database model for deployment, with the application operating on a Windows based system for data storage. Distribution of the software includes the V6 software and Microsoft Visual FoxPro Version 7 and 9.

► Note: The V6 software stores encrypted Primary Account Number (PAN) and Expiration Date and does not store sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)) or card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card).

Data Capture and Removal

V6 can accept credit cards through a Verifone PIN pad (1000se), a magnetic card reader or manual entry. V6 may capture the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere), card verification values or codes (the three-digit or four-digit card validation code printed on the back of the card), the PIN/Encrypted PIN block or Primary Account Number (PAN) within volatile system memory of the workstation in which the application is installed. The V6 software stores encrypted Primary Account Number (PAN) and Expiration Date and does not store, and may not be configured to store, sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)), card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) or the PIN/Encrypted PIN block after authorization.

The application automatically deletes the full contents of any track from the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere), card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card), the PIN/Encrypted PIN block and PAN upon authorization from volatile memory.

In the credit card authorization process V6 captures the data, passes it to Medasyst (WnetCard). WnetCard does the authorization and returns the result, at which point the sensitive data is erased from memory. The application will store the authcode and the Primary Account Number (PAN), but does not store sensitive authentication data (magnetic stripe data—located on the back of a card, contained in a chip, or elsewhere), card verification values or codes (the three-digit or four-digit card validation code printed on the back of the card), or the PIN/Encrypted PIN block anywhere in the system.

Cryptographic Materials

The PAN and expiration dates can be stored in data tables at the IMS level for accounts receivable purposes. These are stored in compliance with the PCI guidelines utilizing 256-AES encryption. The magnetic stripe data—located on the back of a credit card, contained in a chip, or elsewhere—is not stored to permanent media, i.e. hard drive. Other sensitive data, such as the 3 or 4 digit card validation code, PIN, and CVV, are not stored to permanent media.

Keys are generated using 256-bit (AES) encryption using Cypher Block Chaining. These are decrypted in a proprietary process before being handed to the next encryption algorithm. The application supports the merchants' ability to change the key for stored data, the IMS requires that the user present the current key and then create a new key twice, then enter a verification code that changes on each attempt. Two partial keys are stored in a keys table one of these keys are stored with the encrypted PAN. There is an additional record level key with the PAN. These are partial keys that can only be decrypted with another portion of the key from the proprietary software. Decryption requires a two-step decryption bringing three keys together at each step. All pieces are required to decrypt the PAN data.

As the merchant, decide to retain cardholder data in an electronic means outside of the application using third party methods, must ensure to meet PCI DSS requirements for the secure storage of this data and adhere to the cryptographic key management guidelines identified in the latest PCI DSS standard.

Data Purging

As previously stated, the V6 software stores encrypted Primary Account Number (PAN) and Expiration Date but does not store and may not be configured to store cardholder data (sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)), card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) after authorization. Credit Card Capt files will only hold history for the last 30 days. When the file is two days old the encrypted card number and expiration date will be removed. As such, there is no need, as the merchant, to purge cardholder data from the application. However, as the merchant may decide to retain cardholder data outside of the V6 software using third party means (Excel spread sheet, written hardcopy, etc.), must understand that any cardholder data collected exceeding the defined retention period must be purged based upon business, legal, and/or regulatory requirements in order to achieve and meet own PCI DSS compliance requirements.

Historical Data

Previous versions of the software do not store, and may not be configured to store, sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) after authorization.

As with the current version, previous versions automatically delete the full contents of any track from the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) upon authorization from volatile memory.

Credit Card Capt files will only hold history for the last 30 days. When the file is two days old the encrypted card number and expiration date will be removed.

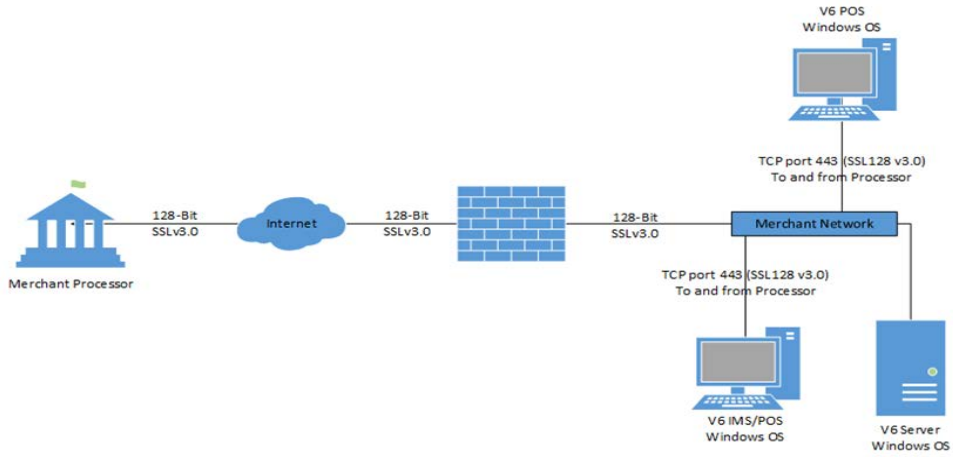
Deployment

This section describes the proper deployment for the V6 application and its underlying systems supporting the application and its database. It is imperative that these directions be followed, as they are designed to achieve PCI DSS compliance. Following the guidelines within this section does **NOT** make the customer PCI DSS compliant, nor does it guarantee network's security. It is the customer's responsibility to ensure that hardware and network systems are secure from internal as well as external threats. While this guide will go over the requirements the customer will need to follow for the implementation of V6 that will help achieve PCI DSS compliance, it is solely the customer's responsibility to ensure the proper implementation of the application.

AcuSport makes no claims on the security of the customer's network, nor of the level of PCI DSS compliance.

Recommended Network Deployment

The typical V6 deployment consists of one or more Microsoft Windows workstations running the POS and/or the IMS and/or one Microsoft Windows server machine, running the database software. The application communicates with the processor over the Internet using HTTPS (TCP port 443) for authorization and payment capture. Therefore, an Internet connection is required. This Internet connection must be protected by a firewall, as neither the application nor the database is permitted to be directly connected to the Internet, per PCI DSS requirements. The firewall must allow the outbound HTTPS (TCP port 443) access to the processor. However, the firewall must be configured to not allow any Inbound Internet access to the workstations supporting the V6 application or to the database. Allowing inbound Internet access to these systems, it will compromise PCI DSS compliance. A simple diagram of a standard deployment is shown below:



► Note: PCI DSS requires that cardholder data must not be stored on Internet accessible systems, nor can a server containing cardholder data be located within an Internet accessible network. A firewall must be deployed at each Internet connection and configured to prohibit "Inbound" Internet access to systems supporting the application and its supporting database.

Required Services, Protocol, and Dependent Software & Hardware

The V6 software requires Microsoft's Visual FoxPro Version 7 and 9 and Chilkat software for data storage. This software is provided and installed with the application distribution package.

The V6 software communicates over the TCP/IP protocol suite for functionality. The application utilizes HTTPS (TCP port 443) to communicate with supported processors over the Internet for authorization and payment capture. Additional ports are needed for the following processors TSYS port 5003, WorldPay port 6660, and Heartland Payments System port 22342. In conjunction with the ports the processor URLs can be used Elavon URL webgate.viaconex.com, FDMS URL vxn.datawire.net, CHASE Paymentech URL netconnect.paymentech.net, Global Payments East URL igusproda.globalpay.com, TSYS URL ssl2.vitalps.net, WorldPay URL tptrans.lyksystems.com and Heartland Payments System URL sslprod.secureexchange.net.

- Note: Allowing only destination to the processor's URL would prevent users from accessing the internet for non-credit card related functions.
- Note: Communication with the processor only requires Internet outbound HTTPS (TCP port 443) access. No Internet inbound access of any type is required for functionality. It is recommended to disallow all Internet inbound access to the POS software. PCI DSS requires to disallow all Internet inbound access to the database. Failure to do so will jeopardize PCI DSS compliance.

As previously stated, the application only requires the use of the TCP/IP protocol and the HTTPS (TCP port 443) and TCP ports 5003, 6660, 22342 for functionality. These are the only protocols and services enabled by default "out-of-the-box". No unnecessary or insecure services, daemons, protocols or components are enabled by default by the application on supporting systems or the application, nor are any required by the application to function properly.

V6 supports the use of Verifone 1000se PIN Pad for processing debit cards.

Third Party Software Requirements

- VFP version 7 and version 9 (http://msdn.microsoft.com/en-us/vfoxpro/default.aspx)
- Medasyst WnetCard (http://www.medasyst-software.com)
- Dynazip (http://www.innermedia.com)
- XFRX (http://www.egeus.com/frx2wrd.php)
- Chilkat (http://www.chilkatsoft.com) 32-Bit ActiveX Components

Third Party Resellers and Integrators

- Total Registers Systems (http://www.trs-pos.com)

Application Components

- Medasyst WnetCard handles the credit card processing to and from the processor.
- Dynazip handles zip and unzip of files.
- XFRX handles report generation for PDF, Excel and HTML.
- Chilkat handles AES credit card encryption, web service communications, zip, unzip, XML parsing and FTP communication.

Preventing Inadvertent Cardholder Data Capture

For workstation deployments hosting the V6 software, it is important that the following two (2) operating system settings be implemented to ensure that cardholder data is not captured by the operating system itself, as this may compromise PCI DSS compliance.

The merchant will want to disable memory page swapping to the hard drive. The following steps will show how to tweak virtual memory settings in Windows by disabling (pagefile.sys).

1. Open **Control Panel > System and Maintenance > System**.
2. In the left "Tasks", click on **Advanced System Settings**.
3. The "Advanced" tab should display. In "Performance" section, click on **Settings** button.
4. Click on **Advanced** tab.
5. In the "Virtual Memory" section, click on **Change** button.
6. By default, "Automatically manage paging file size for all drives" setting is selected so that the Windows system can manage the paging file without a user being interrupted. To change the paging file size, move the pagefile.sys to another drive, or disable virtual memory paging, uncheck the check box of **Automatically manage paging file size for all drives**.
7. Select and highlight the appropriate drive to change the paging file settings under the box of "Drive [Volume Label]". For the workstations this would be the "C:" drive (the only drive available).
8. To disable paging file or virtual memory, simply click the "no paging file" radio button and then click the "OK" button.

The following steps will show how to disable system restore points. This is critical as a system restore point may inadvertently capture cardholder data if it is not disabled and can compromise PCI DSS compliance.

1. Access workstation's system properties.
2. In the **System Properties** dialog box, click the **System Restore** tab.
3. Click to select the **Turn off System Restore** check box. Or, click to select the **Turn off System Restore on all drives** check box.
4. Click **OK**.
5. The following message will display: "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 computer. Do you want to turn off System Restore?", click **Yes** to confirm to turn off System Restore
6. After a few moments, the **System Properties** dialog box closes.

Transmitting Cardholder Data

V6 application transmits cardholder data over the Internet using 128-bit SSL 3.0 for encryption to the processor. This is done by default and cannot be disabled. This secure, encrypted transmission is required to maintain PCI DSS compliance. This is the only means of transmitting cardholder data supported by the V6 software; the application does not support and/or facilitate sending of PANs by end-user messaging technologies.

The authentication settings for transmitting credit card data (CC Processor, Modem Port and Init String) are configured in CC Setup screen under Properties and stored in the database. The setup screen is only accessible to a PCI user with a security role.

► Note: Understand that the transfer of cardholder data across public networks must be encrypted in order to maintain PCI DSS compliance.

Installed Files

The V6 software is installed using Visual FoxPro technology. The following applications are installed:

- IMS
- POS

The installed files are located under C:\arsapps\ars5\ims5 and C:\pos5 folders.

Display of the PAN

The V6 software does not allow the full PAN to be displayed anywhere in the system other than upon initial manual entry and in Sales Orders and AR Customer after the single card number is decrypted for viewing.

The PAN is masked (by either displaying only the last 4 digits or the first 1 and the last 4) by default on all outputs.

Application Versioning Methodology

V6 version number follows an industry standard consisting of three segments delimited by a ".": Major.Minor.Build. Only Major, Minor and Build version numbers are published.

Major Version

Major version doesn't change.

Minor Version

Minor version changes when there is a significant change in architecture or addition of features that may impact the security posture of the product such that a review of the product may be required through an internal or external audits such as PA-DSS or other third party security/risk assessment or impact due to change in the application that is affected by an external compliance requirement (PA-DSS).

Build Version

Build version (service pack) changes when there is a collection of changes to the application that identify, fix, test and release minor software defects, which can include various bug fixes or new features. In such circumstances the build number updates sequentially each time one of the changes is required. This number resets to zero upon making the next Minor build of software. The changes usually do not impact the architecture of the application and would normally not require a security audit like PA-DSS.

Software Development Life Cycle

AcuSport uses the Agile Life Cycle Method of Development. We are currently in a maintenance phase of our Inventory Management and Point of Sale products. When new development occurs, we break the projects into small modules. Each iteration goes through stages of analysis, design, production, testing and documentation. The small changes in the products then accumulate over several weeks until we have enough in volume or in importance to justify another build version.

Details of the Development Process

We perpetually receive requests from our customers and support staff to modify our products. This can be a module enhancement, a bug fix, or new modules. This results in a pool of requests that are then evaluated by management. After evaluation, some work items are approved to go into the system. This is followed by the projects being prioritized and broken up into tasks. We assign the tasks to various developers that work on individual tasks until they can be tested and reviewed between the development team. This continues until there is enough for our support staff to independently test the changes. After evaluation from support, if necessary, we rework any problems, test, and send it back to support. This happens until it satisfies the initial request and is error free. Once we pass this point, we document in our build notes what the change is, and if it was a bug, what it fixed. After we gather a few of these, or it is a critical fix, we then release the build version into production to be available to our customers to update their system.

Details of the Testing Process

There are several phases of testing. First when the original developer is altering the system, there is perpetual testing to ensure that it is bug free and the logic is correct. After the original developer is finished, the development manager is notified and then it is reviewed. After this is satisfactory, then the development team collectively meets to review the change, providing input and suggests any necessary modifications. This cycle occurs until complete.

The next phase is to hand off the pre-production version to our support department for them to test the changes and other random areas in our programs. Again, if any changes are needed, we complete the cycle again. When the modification affects the payment module, the development department does not test with live data. Depending on what the change affects, we determine if we are able to test and if so, we test as much as possible. The development department never accesses the payment module in the manner where it will utilize its gateway to the payment processor. This is only done by the support department.

The support department uses test data and accounts to test the functionality of the payment module. There are times that the support department is testing a functionality that requires a real account. In this case we use our company's merchant account with our company's business card, charging a small amount sale and then using the return

function to reverse the sale. This is done with a pre-production version until we are satisfied that the functionality works. Once this is finished and approved, we then release the program into production. The production version is never released with data associated to the payment module.

Separating Development/Test Code from Release Code

Our development environment is used to modify the existing products and only test as it is being developed for debugging and logical conformity. With regards to the payment module, the development department does not test with live data, nor does it access the payment processors via the payment module's gateway. We leave that up to the support department during its testing phase.

The physical locations of the development environment and production environments are never on the same servers or workstations. The product development occurs on one server and does not contain any live production data. With regards to the payment module, it does not contain any data. These servers are called "ASPTH046" (development), "ASPTH047" (production). Neither are exposed to external internet traffic and are both behind a firewall.

Support and QA use local workstations, within a local network, to test the functionality of the product changes. The support and QA use test data and accounts to test the functionality of the payment module. There are times that the support department is testing a functionality that requires a real account. In this case we use our company's merchant account with our company's business card, charging a small amount sale and then using the return function to reverse the sale. This is done with a pre-production version until we are satisfied that the functionality works. Support only uses batching to verify that all aspects of communication are correct. After this is finished, we erase the supporting files and any data files that have collected payment information.

Once this is finished and approved, we then release the program into production. Additionally, the production version is never released with data associated to the payment module. The production environment used for our own payment processing is on "ASPTH047" server. Again, this is not directly connected to the internet, rather is part of a local network. Being a POS company, the other production environments are maintained by our customers off-site from AcuSport.

Wireless Networks

V6 is not a wireless application and has not been developed to use wireless technology. As such, it does not require a wireless network and is not written to operate on mobile devices. Furthermore, the application is not bundled with applications requiring wireless connectivity. Recommended deployment of the application and systems supporting the application is through a wired network.

Choosing to deploy a wireless network infrastructure to support communications between deployed systems, or connect a wireless network to the environment supporting the V6 application, must do so in a manner compliant with the current PCI DSS standards. The secure deployment of a wireless network is solely the customer's responsibility. In order to achieve PCI DSS compliance, the following guidelines must be followed for deployment of a wireless network:

- Wireless encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions;
- Default SNMP community strings on wireless devices must be changed;
- Default passwords/passphrases on access points must be changed;
- Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks;
- Other security-related wireless vendor defaults must be changed, if applicable; and
- Wireless networks transmitting cardholder data or connected to the cardholder environment must use industry best practices to implement strong encryption for authentication and transmission;

If wireless network deployed within environment and it is not part of cardholder network, a firewall is required between any wireless networks and the cardholder data environment. The firewall must be configured to deny or control any traffic from the wireless environment into the cardholder data environment.

Access

User Access controls are an important requirement to maintain PCI DSS compliance. User access controls must be implemented at the system (O/S), database, and application level.

For the application and the supporting database, each user must have their own unique user ID. During the initial installation, a new user is created for the application that can be then used to create other accounts. For the database, all default accounts should be disabled upon install and must remain disabled or will compromise PCI DSS compliance. Individual users must not share accounts, as this compromises accountability, as all activity performed by a user of the application is tied to their individual user ID.

To create a new user within the application, access the "Security" option and select "New". This will bring up a new window. All the required fields will need to be filled out. After creating the user, the password must be set for the user. This is done by selecting the employee that was just created and going to "Change Password". The user ID can be changed or the password set for the user.

The password policy for non PCI users can be set up by going to the "Properties" option and selecting "Apply PCI Compliance Strict Password Rules".

A PCI user that has access to CC Setup (PCI role) or Audit Log (PCI role) must meet the following conditions:

- Password length must be no less than seven (7) characters (PCI DSS 8.5.10); and
- Passwords must be a combination of numeric and alphanumeric characters (PCI DSS 8.5.11).

The following password controls are enforced on PCI users that have PCI role:

- A minimum history of the last four (4) passwords is maintained (PCI DSS 8.5.12); and
- Passwords expire every ninety (90) days (PCI DSS 8.5.9).

The following user lockout and session controls are enforced on users that have PCI role:

- Accounts are locked out after no more than six (6) failed login attempts (PCI DSS 8.5.13);
- A minimum lockout duration of thirty (30) minutes is enforced (PCI DSS 8.5.14); and

The following user session controls are enforced on all users:

- A session time out after fifteen (15) minutes max is enabled (PCI DSS8.5.15).

All IMS user passwords are stored in the database and are SHA256 hashed prior to transmission and storage and also encrypted.

POS uses personal identification numbers, and they are store unencrypted in a clerk file. The POS users only have access to single card number for the sale/return and the

settling of the credit card batch. The credit card batch only prints out first digit and last four digits of the PAN.

For the underlying systems and the database, it is imperative to implement the same user and password controls as those established for the V6 application. Failure to do so will compromise PCI DSS compliance. As such, the user must use the inherent user, password, and lockout controls for the underlying systems and database to ensure the following is accomplished for every user of the database or supporting systems:

- Assignment of unique user IDs for any created user account (PCI DSS 8.1);
- No default accounts may be used and all must be disabled or removed;
- User accounts must not be shared by users;
- Use of passwords, passphrases or two-factor authentication is required for each created account (PCI DSS 8.2);
- No group passwords are allowed, and generic User IDs and accounts are not created or used by the application, nor should they be created by the merchant and are to be disabled or removed (PCI DSS 8.5.8);
- Passwords expire every ninety (90) days (PCI DSS 8.5.9);
- Password length must be no less than seven (7) characters (PCI DSS 8.5.10);
- Passwords must be a combination of numeric and alphanumeric characters (PCI DSS 8.5.11);
- A minimum history of the last four (4) passwords is maintained (PCI DSS 8.5.12);
- Accounts are locked out after no more than six (6) failed login attempts (PCI DSS 8.5.13);
- A minimum lockout duration of thirty (30) minutes is enforced (PCI DSS 8.5.14); and
- A session time out after fifteen (15) minutes is enabled (PCI DSS 8.5.15);

Logging

A key feature of V6 to meet PCI DSS compliance is logging. V6 enables extensive logging for all user types. This logging (Audit PCI table) is required to maintain PCI DSS compliance and, as such, logging is enabled by default per PCI DSS and PA DSS requirements and may not be disabled or configured.

Log File Location and Names

POS log files are located under the application within the V6 POS install directory (C:\pos5). The following log file can be found:

- errors.htm - This log captures errors for the POS application

The following logs are available in the VFP database:

- Event Log - This is a table in the VFP database to store errors for the IMS application.
- PCI Audit Log - This is a table in the VFP database to store various actions taken by the user:
    - All actions taken by user in the credit card setup.
    - Access to audit trails.
    - All actions taken by any individual with root or administrative privileges (security management (roles, ID and Password changes) or credit card set up).
    - Use of identification and authentication mechanisms.
    - All elevation of privileges.
    - All changes, additions, or deletions to any account with root or administrative privileges.
    - Application updates

Viewing Log Files and Exporting

The logs within the VFP database can be viewed by going to PCI Audit Log or Event Log under Utilities menu. PCI Audit Log can only be used by users who are part of the PCI role. The log files can be viewed by going to the V6 IMS/POS install directory and opening the files.

File Monitoring

V6 has a set of files and sub-directories that must be monitored for modification attempts.

- C:\arsapps\ars5\ims5\data\ar.dbf
- C:\arsapps\ars5\ims5\data\config.dbf
- C:\arsapps\ars5\ims5\data\keys.dbf
- C:\arsapps\ars5\ims5\data\pconfig.dbf
- C:\arsapps\ars5\ims5\data\soctlg.dbf

- C:\arsapps\ars5\ims5\data\users.dbf

Remote Access

The V6 application does not support remote access capabilities. However, the underlying Windows Operating System (O/S) does support remote access. The customer, as a merchant, may choose to utilize these remote access capabilities, but in order to maintain PCI DSS compliance only remote access technology supporting two-factor authentication may be used. Two-factor authentication consisting of something to have, know, or are is required for remote access in order to maintain PCI DSS compliance. In addition to the use of two-factor authentication, it is important to remember that the remote access capability should only be enabled when needed and disabled when no longer required. Furthermore, remote access software must provide the following features or configuration settings:

- Must ensure changes are made to the default setting in the remote access software;
- Remotes access software must be configured to only allow access from specific IP addresses;
- Encrypted data transmissions such as IPSEC VPN, SSH, 128-Bit SSL v3.0 must enforced;
- Access to customer passwords must be restricted to authorized personnel;
- Logging of remote access must be enabled;
- Systems must be configured so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed;
- Unique user IDs must be used for each user account;
- Authentication composed of passwords and two-factor authentication must be used for remote access;
- Remote access must not require or use any group, shared, or generic accounts or passwords;
- Passwords must change every ninety (90) days or less;
- Passwords must be a minimum of seven (7) characters;
- Passwords must contain both numeric and alphabetic characters;
- Password history of the last four (4) passwords must be kept and new passwords must be different than any of the last four (4) passwords;
- Account lockout must occur after six (6) invalid logon attempts;
- Remote access accounts must be locked out for no less than thirty (30) minutes or until reset by a system administrator; and
- Remote access sessions must timeout after no more than fifteen (15) minutes of inactivity.

► Note: All remote non-console administrative access to the payment application or servers in the environment must be encrypted utilizing SSH, VPN, SSL/TLS or other encryption technology in order to maintain PCI DSS compliance

In the case of AcuSport customer support, AcuSport utilizes the application Bomgar for remote access with one time tokens for each access instance that is provided by the merchant and is unique for each access. The Bomgar support is installed on the system

during the initial application install. Bomgar can be enabled or disabled at any time. The merchant can grant users access by typing in a random password on the support website or by granting a “yes” permission through a popup when customer support is connecting.

Software Upgrades

The V6 application is installed using Application Manager and software upgrades are made available the same way. Each application is installed from the V6 Application Manager.

Each application checks for available updates on startup. If an update is available, it will need to be downloaded and installed manually. Should the merchant need assistance in applying an update, may contact AcuSport support staff at: 800-547-7120.

► Note: Remember, when the computer in use is connected via VPN or other high-speed connection, a firewall or personal firewall must be utilized to secure these "always-on" connections.

Support

Customers may contact AcuSport for support in troubleshooting their V6 application or for the reporting of issues with the application. AcuSport support consists of phone and, when needed, remote access support. AcuSport support may be contacted at:

Phone: 1-800-547-7120

Email: RTGSupport@AcuSport.com

► Note: AcuSport will not collect sensitive authentication data (magnetic stripe data, card validation codes or values, and PINs or PIN block data) or Primary Account Numbers (PAN) for any reason, even upon customer request. To do so may compromise AcuSport's PA DSS validation for V6 and, in return, PCI DSS compliance.

As a customer, deciding to collect sensitive authentication data as part of own troubleshooting process, must adhere to the following guidelines or risk compromising PCI DSS compliance:

- Must only perform the collection of sensitive authentication data when needed to solve a specific problem;
- Store such data in a specific, known location with limited access;
- Must perform collection of only the limited amount of data needed to solve a specific problem;
- Must provide for the encryption of sensitive authentication data as required upon storage; and
- Must perform secure deletion of such data immediately after use, using tools which utilize the DoD 5220.22-M military grade secure deletion process.

Revision

The revision section of this guide will itemize changes and updates made to the guide as they relate to application changes or updates that impact the PA DSS requirements, or as needed per updates to the PA DSS requirements themselves. At a minimum, the guide is reviewed annually to ensure its completeness and adherence to the current PA DSS standards. In addition, the guide is reviewed and updated as needed after each release of the evolving PA DSS standards, to ensure compliance with the current PA DSS. Finally, this guide is reviewed and updated after changes or updates to the application itself that impact the PA DSS requirements or information contained within.

The table below contains an itemized list of changes to this guide:

Document Version #	Description of Change
1.0	Initial Release

Updates to this guide will be delivered to each customer's registered point of contact with a summary of changes and discussing possible impacts to deployment or environment. These same updates are available through the AcuSport support site for registered customers. All AcuSport customer support staff are trained on any updates to the application and implementation guide prior to the release of the application. Should further explanation be required, customers may contact support at 800-547-7120.