



PA-DSS Implementation Guide

InFusion™ Version 3.50

ParTech, Inc



PA-DSS Implementation Guide

Documentation Comments	This document was developed by ParTech, Inc. For content revisions, questions, or comments, contact the writers at PTI.Compliance@partech.com .
Copyright	This product and related documentation are protected by copyright and are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form by any means without prior written authorization of ParTech, Inc.
Version	Version 3.50 February 2009 Effective on the Date of General Release for Version 3.50 Printed in USA
Trademarks	InFusion, PAR, and the PAR logo are all trademarks of PAR Technology Corporation. ParTech, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from ParTech, Inc., the furnishing of this document does not give you any right, title or license to these patents, trademarks, copyrights, or other intellectual property. Other product names may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Disclaimer	ParTech, Inc. has reviewed this document, and it is believed to be reliable. However, this document is provided for informational purposes only and is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, any warranty of merchantability or fitness for a particular purpose. ParTech does not make any warranties or representations that the information contained in this document will meet your requirements or will be error free. The entire risk of the use or the results of the use of the information contained in this document remains with you. This document is subject to change without notice.
Revision	This document is reviewed annually and updated based on any major or minor InFusion software changes as well as with changes to the PA-DSS requirements.
Technical Support	Technical Support is available to the end user with a valid support contract or by a per call billing provided by ParTech, Inc. Customer Support Center. ParTech, Inc. Web site www.partech.com
Contact	ParTech, Inc. 800-448-6505 Direct New Hartford, NY



Table of Contents

Table of Contents	3
Change History	3
Forward	4
System Accessibility	5
Internet Connectivity and Security	6
Data Retention	7
Web-Based Applications	7
Wireless Implementation	8
Remote Desktop Support & Management	9
Network Security	9
Historical Clean-Up	10
Upgrading Older Systems	10
Securely Deleting Files	10
Troubleshooting and Data File Handling	10
Glossary	11

Change History

Revision	Reason for Change	Changes	Date
A	Initial Release		03/23/09
B	PCI DSS 1.2.3 and annual review statement		05/11/09



Forward

The Payment Card Industry Data Security Standard (PCI-DSS) and the Payment Applications Data Security Standard (PA-DSS) define specific requirements for all organizations that store, process and transmit cardholder data. Further information regarding either is available at the following websites:

<http://www.pcisecuritystandards.org/>

http://usa.visa.com/merchants/new_acceptance/accepting_visa.html

With the release of InFusion™ Suite Version 3.50 and higher (“InFusion”), you have the ability to configure InFusion to utilize the security functionality to protect all sensitive credit data, as outlined in the Payment Applications Data Security Standard Guidelines. If you utilize the security functionality, all sensitive credit data within the system will be secured. However, in addition to utilizing the security features within InFusion, there are several key actions you can take to further secure the data within each of your locations. All statements are made to help you achieve PCI DSS compliance. If any statement is made which would affect your PCI compliance the PCI DSS 1.2 guidelines should be referenced as the ultimate authority on the topic.

The following is a list of recommended key actions.

System Accessibility

InFusion requires each user to have a unique user ID and password in order to access the system. However, along with this, the following combination of OS access controls and InFusion recommendations should be applied.

- The default Supervisor's manual entry number must be changed from its initial setting, replacing it with a magnetic swipe card or complex manual entry number.
- The default manual entry number for all InFusion's utilities must be changed.
- Ensure that the end-user is never verbally provided or can see the use of a manual entry number by the support technician, either in person or during remote dial-in.
- Magnetic swipe access should be the only methods of POS access provided to staff capable of closing or authorizing transaction functions on a guest check.
- Do not re-use employee swipe cards. The employee swipe card should be returned. The former employee's record must be set as 'Inactive' and delete the badge number field in the InForm employee database.
- Do not use group, shared or generic accounts and passwords.
- PA-DSS compliant complex passwords require the following criteria:
 - They are at least 7 characters in length.
 - They contain both upper case and lower case letters.
 - They contain numbers and (if possible) special characters.
 - Change user passwords at least every 90 days.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or under.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password or re-activate the terminal.
- Disable guest accounts to any server. Only accounts with authorized usernames and passwords should be granted access to any application.
- Changing compliant settings will result in non-compliance with the PCI DSS.

For further information and recommendations, refer to the PCI Security Standards Council's Requirements documentation.

Internet Connectivity and Security

Having secured the database and related files if any one of your sites has an internet connection, the following recommendations should be applied.

- Internet firewall protection is required.
- Anti-virus software is required with routine updates to the virus definitions.
- Staff must be restricted from having any Internet access.

All unnecessary services should be disabled on the back office server and terminals. The firewall that protects the back office server should have a very restrictive set of rules.

For more information and recommendations, refer to the PCI Security Standards Council's Requirements documentation.

Located on the following link are three guides for Windows XP Professional and Windows 2003. You will need to follow all of them in order to achieve Evaluation Assurance Level (EAL) 4 [CC certification is an international standard for ensuring that IT products conform to stringent security requirements.]. The guides are:

- Administrator's Guide
- Configuration Guide
- User's Guide

<http://www.microsoft.com/technet/security/prodtech/windowsxp/cc/default.msp>

Data Retention

It is recommended that the system only retain essential information long enough to reasonably support credit card transactions. The storage of cardholder information is located on the back office computer in c:\partech\rms\log*.pay and on backup terminals in the c:\rms\log*.pay.

InFusion's payment log files do not contain any sensitive data.

- PCI-DSS requirements state that you should employ a backup procedure that archives and stores all security logs for at least one year.
- You should consider using Windows auditing at all of your locations to track activity in the following directories:
 - \partech(and sub-folders)
- On POS Terminals
 - \
- Other logs
 - Antivirus/Malware
 - Routers/Switches
 - Firewall Appliance
 - Folders storing 3rd party credit card software (such as PCCharge, Monetra, etc.).
- InFusion employs PCI-DSS compliant logging by default. Disabling any of these logs will result in a non-compliant application.
- It is required that the customer establish and maintain PCI DSS-compliant logs to include:
 - Individual accesses to cardholder data
 - All actions taken by any individual with root or administrative privileges
 - Access to all audit trails
 - Invalid logical access attempts
 - Use of identification and authentication mechanism
 - Initialization of the audit logs
 - Creation and deletion of system-level objects
 - User identification
 - Type of event
 - Data and time
 - Success or failure indication
 - Origination of event
 - Identity or name of affected data, system component, or resource
- Not establishing these logs will result in a non-compliant system.

For instructions on how to configure Windows auditing, refer to the following website:

<http://technet2.microsoft.com/windowsserver/en/technologies/featured/audit/default.mspx>

For more information, refer to PCI Security Standards Council's Requirements documentation for log settings.

Web-Based Applications

InFusion has no web-based applications as part of the product offering.

Wireless Implementation

A wireless network is never allowed to access the cardholder data environment. There should be appropriate firewalls separating these two networks and must be configured to deny or control any traffic from the wireless environment into the cardholder data environment (PCI DSS requirement 1.2.3). For locations with wireless connectivity to the back office server, industry standard WPA2 security is recommended. If there are any questions regarding Visa standards for wireless security, refer to the PCI Security Standards Council's Requirements documentation (PCI-DSS 1.2 Guidelines).

You should consider the following:

- Ensure that firewall protection is available on a Wireless Access Point and any of your PCs connected to the wireless network including mobile and personal devices such as laptops.
- Connect wireless access points to a switch port, not a shared device (such as a hub).
- Use one of the following encryption methodologies: WPA or WPA2. Others such as VPN, 128bit SSL/TLS and 128bit WEP can be used provided an additional methodology is in use to protect the data (such as RADIUS).
- For automated key rotation processes (LEAP), key change every 10-30 minutes.
- All management of wireless environments should only be from the console.
- Ensure any wireless virus signatures are included in the virus protection mechanisms.
- Disable file-sharing on all your stations (not PosServer).
- Restrict access to the wireless access points by MAC addressing.
- Change encryption keys from the default settings any time someone with knowledge of the keys changes positions or leaves the location.
- The default SSID (Secure Socket ID) is changed and broadcast if the SSID is disabled.
- The default SNMP community strings and passwords on access points are changed.
- Use static IP addresses on wireless access points.
- Logging and Auditing must be enabled.
- IDS must be applied to the wireless network.
- Physical access to gateways, access points and handheld devices is appropriately restricted.
- Locate the access points as close to the center of the facility as possible to minimize the distance that the signal needs to travel.

All wireless applications must adhere to the standards defined in the PCI Data Security Standard.

Remote Desktop Support & Management

If employees, administrators or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. Establish and utilize a secure, encrypted methodology for remote desktop support and management utilizing the following recommendations:

- If Remote Desktop Protocol (RDP) takes place over a public network or via RAS connection, the session should be encrypted.
- Usernames and complex passwords (2-factor authentication) should be required for all remote access to the POS system.
- The RDP host software should only be run when needed when connectivity takes place over a public network or RAS connection.
- The required approach is to use a 2-factor authentication for user login to the remote access software site, such as the use of a serial ID as used in pcAnywhere version 10+. This serial ID is in addition to the username and complex password.
- InFusion will work with RADIUS and VPN data protection.

Network Security

Please refer to the PCI Security Standards Council's Requirements documentation for guidance on network security and Microsoft's guides for Windows configuration on the following link:

<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/ccc/default.msp>

InFusion does not configure your networks and does not provide instructions for network configuration and maintenance. Below are three main points for consideration:

- For any configuration that may require data transmission over the internet, Secured Socket Layer (SSL) protection is required.
- For remote access, it is required that the location has firewall protection and implemented security procedures that utilize individual user IDs and passwords. It should also have a very restrictive set of ACLs or rules for access.
- All unnecessary and insecure services and protocols (such as unencrypted FTP) should be disabled. If such services are required, you should ensure that such services are encrypted.

Historical Clean-Up

InFusion 3.50 on upgrade will remove all existing credit card information from the server. It is recommended that you perform a backup of the POS prior to upgrading.

Upgrading Older Systems

If you are upgrading an existing InFusion site from version 3.x, then you will need to do the following:

- Backup your current database.
- Upgrade the InFusion software to version 3.50+
- Backup your upgraded database.

If the InFusion system is integrated with 3rd party software, it may be necessary to identify whether an upgrade of those files is required. It is also possible that the current version of that software may have log files which are retaining sensitive data (such as the log files from a credit card verification system). Research which (if any) files need to be cleared and whether an upgrade to that software is required for PA-DSS compliance.

Securely Deleting Files

To securely delete files and or old data files which may contain sensitive cardholder data, a tool such as Eraser should be used. Eraser is an advanced security tool (for Windows), which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected pattern. This tool is available from <http://www.heidi.ie/node/6>.

Troubleshooting and Data File Handling

- Collection of sensitive authentication only when needed to solve a specific problem.
- Store collected data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete collected data immediately after use.

Glossary

Backup	A duplicate copy of data made for archiving purposes or for protecting against damage or loss.
Cardholder	The customer to whom a card has been issued or the individual authorized to use the card.
Complex Password	A password of at least 7 characters with both numeric and alphabetic characters. Preferably (where applicable) with special characters as well. Complex passwords should be changed every 90 days.
DMZ	Demilitarized Zone is a part of the network that is neither part of the internal network nor directly part of the Internet. It basically sits between the two.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (inverse to encryption) against unauthorized disclosure.
Firewall	Hardware and/or software that protects the resources of one network from users from other networks. It prevents outsiders from accessing the system's private data resources.
HTTPS	Hypertext Transfer Protocol Secure. This enables the secured transmission of web pages.
IP Address	A numeric code (Internet Protocol address) that uniquely identifies a particular computer on the Internet. A "Static" IP address is one that is assigned to a specific PC and never changes.
Key	In reference to encryption, a key is a value applied using an algorithm to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
Magnetic Swipe	A card encoded with a magnetic stripe which contains data identifying the cardholder and other pertinent data. Employee access cards are one example of magnetic swipe cards in which the cardholder logs into the POS. Credit cards are another example of magnetic swipe cards which identify the cardholder's account number and other private information.
Manual Entry Number	Access to InFusion POS is possible by applying a numeric access code. It is not as secure as the Magnetic Swipe or Bio-Metric scan methods.
Password	A string of characters that serve as an authenticator of the user.
SSL	Secured Socket Layer. Allows encrypted files to be transferred from computer to computer using a private key to code data that is sent over SSL connections.
Virus	A program or string of code that can replicate itself causing the modification or destruction of software or data.
WPA	Wi-Fi Protected Access is a new standard for wireless networks (considered more secure than WEP).