ChargeItPro
A Payment Processing Partners Product

Implementation Guide

Payment Card Industry
Data Security Standard 2.0

Guide version 4.0

Table of Contents

Important Note: Industry Organizations and Third-Party Software

Throughout this guide we refer to industry resources and providers of security related products that can help you comply with PCI DSS requirements. This information is provided for your convenience only. Payment Processing Partners does not own, control, endorse, or specifically recommend any of the products or vendors mentioned. A listing of Web sites for these organizations is included at the end of this document.

Overview

Thank you for choosing ChargeItPro as your payment processing solution. We value our relationship and want to provide you with important information about the installation and operation of your ChargeItPro software.

This implementation guide is provided to assist you in complying with the Payment Card Industry Security Standards Council (PCI SSC) Data Security Standard (DSS) for protecting payment card data. It is disseminated to the clients, resellers and integrators that process card payments with ChargeItPro.

Note: Not Intended for Card Issuer Use

The ChargeItPro application is not intended for issuers and/or companies that support issuing services and as such does not provide for issuing functionality. As such, ChargeItPro 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 front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)), or the PIN/Encrypted PIN block post-authorization.

What is the PCI SSC DSS?

The PCI Security Standards Council™, formed by the major Credit Card Associations, has issued the Payment Card Industry Data Security Standard (PCI SSC DSS), which includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The PCI SSC DSS applies to merchants and service providers but not to software such as ChargeItPro. It is the obligation of each merchant or service provider to ensure their compliance with the PCI DSS. As the PCI DSS requirements evolve, it is important that you stay abreast of the requirements to ensure your compliance.

The PCI DSS is comprised of 12 general requirements designed to:

- Build and maintain a secure network
- Protect cardholder data
- Ensure the maintenance of vulnerability management programs
- Implement strong access control measures
- Regularly monitor and test networks
- Ensure the maintenance of information security policies

The specific compliance requirements that apply to a merchant or service provider are based on the types of transactions you handle (such as card not present, imprint only, POS system connected to Internet, and so on). Four "validation categories" have been established outlining the requirements for each transaction type and a self-assessment questionnaire is available to help you determine requirements that apply to you. ChargeItPro encourages you to be familiar with these categories and their requirements.

You can learn more about the PCI Security Standards Council, get copies of the PCI SSC DSS documentation, and access the self-assessment questionnaire at their Website. See the Industry Resources section of this document for more information.

Payment Application Data Security Standard (PA-DSS)

ChargeItPro considers the security of cardholder data to be of utmost importance. In developing ChargeItPro, we have made a concerted effort to build a system that will assist you, the merchant, in protecting critical payment card information.

While ChargeItPro is not subject to the PCI SSC DSS, we do fully comply with the Payment Application Data Security Standard (PA-DSS), the PCI Security Standards Council program for software developers that sets guidelines for the design and implementation of payment processing software.

ChargeItPro does not store the following 'Sensitive' data:

- The card's full magnetic stripe data (Track 1 and 2 data)
- Card verification code or value (CVV, CVC, CID data)
- PIN/Encrypted PIN block data from PIN based debit transactions

ChargeItPro stores 'Protected' cardholder data consisting of the primary account number (PAN), and additional cardholder values, including the expiration date and cardholder name using industry standard protection of AES 256-bit strength encryption and is double encrypted after each batch close with a passphrase based public-private key pair. Cardholder account numbers are truncated when displayed on reports or on your screen. The full account number is displayed only to authorized personnel, and only after entering the pre-defined passphrase.

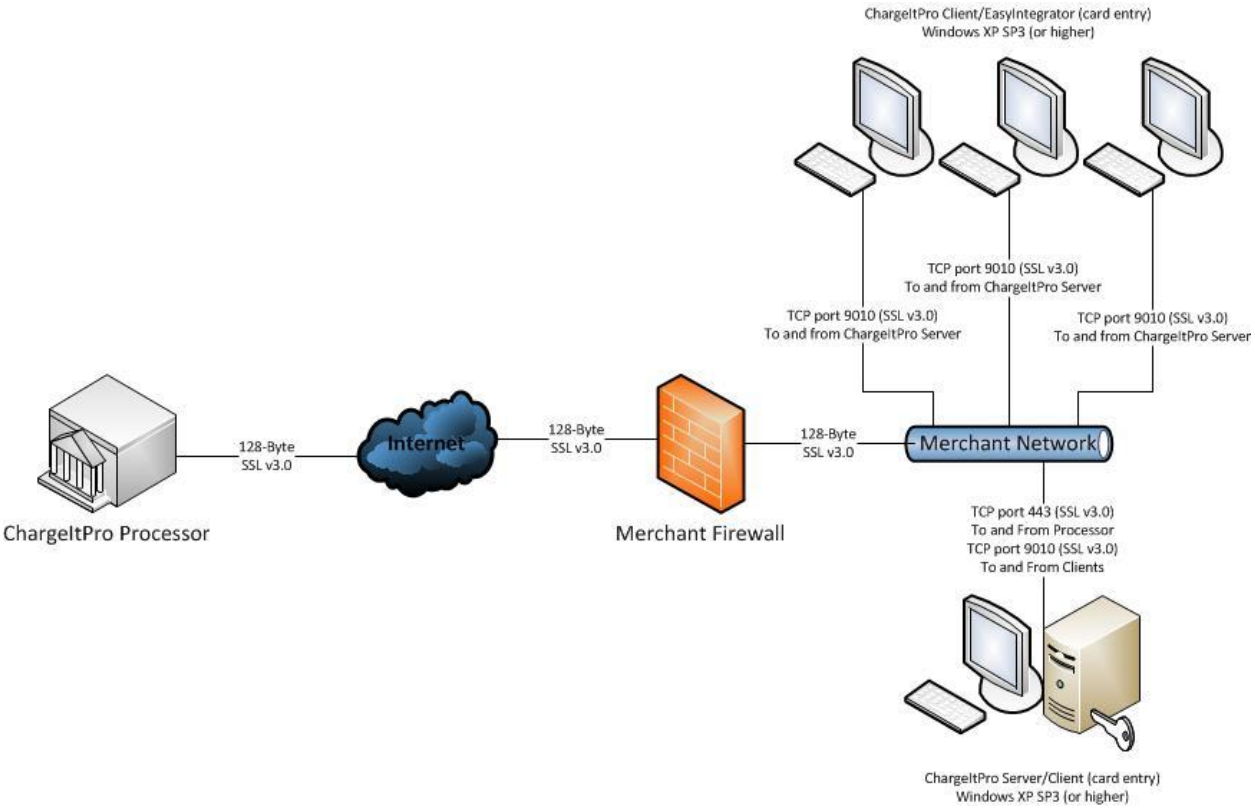
Note: PA-DSS Replaces PABP

Formerly, the PA-DSS standard was known as the Payment Application Best Practices (PABP) and was developed by Visa. With the adoption of this standard by the PCI Security Standards Council, it has been renamed to the Payment Application Data Security Standard (PA-DSS) and applies to all five participating payment cards.

Installation and Implementation

Installation Diagram

The following sample installation diagram represents a typical ChargeItPro installation, highlighting communication between ChargeItPro components and the ports needed for the software to communicate.



Administrative Login

On initial installation the default administrative login is set to:

Login Name = cip

Password = cip

After your first login, you will be prompted to change the administrative login name and password. Select a password that meets the criteria set forth below.

User Accounts

ChargeItPro requires all users to use a login name and password to access the system. You should establish a unique login name and password for each user. Logins should not be shared and passwords should be kept secure.

In addition, groups that have access to administrative functions should have the high security option selected and are subject to the following requirements as prescribed by the PCI SSC DSS. We strongly recommend that you set up your system to comply with these requirements for all users of ChargeItPro and also for your Windows operating system and network devices:

- Passwords must be at least 7 characters in length
- Passwords must contain both letters and numbers
- Passwords must be changed every 90 days
- New passwords may not duplicate any of the last four passwords
- Six failed login attempts will result in a 30 minute lockout of the user
- User will be logged out if the session is idle for more than 15 minutes

As you add new users, grant them access only to the features required to perform their duties. Typically, a sales clerk should not require access to system setup areas or sensitive cardholder data. Access to these administrative areas should be strictly limited.

User accounts should be reviewed on a regular basis and users that no longer require access to the system should be removed.

Security Logs

ChargeItPro security logs are enabled by default when the software is installed. These logs are required for PCI SSC DSS and PA DSS compliance, thus no attempt should be made to disable or otherwise modify ChargeItPro logging.

If required the security log can be exported to a comma delimited “CSV” format by an authorized user through the ChargeItPro Server setup module.

Security Key Management

On initial installation of ChargeItPro, you will be prompted to enter a passphrase. This passphrase is used to encrypt the private key of a public-private key pair that is used to encrypt the AES 256-bit key that protects cardholder data (full account number or PAN). The passphrase is required when a user requests to view this customer data.

This passphrase is not stored by ChargeItPro and we cannot recover it for you if it is lost. Keep your passphrase secure. An effective passphrase should be:

- Long enough to be difficult to guess
- Not a direct quotation
- Hard to guess even if the person knows you
- Easy for you to remember

In addition to the passphrase, a unique, secure master password is generated by the ChargeItPro system which is used to secure protected data (full account number or PAN) in open batches, authorization and offline transaction files.

Your passphrase (and thus your master password) should be changed periodically, at least once a year, or anytime it is suspected of compromise. ChargeItPro securely wipes the previous security keys when you change your passphrase or anytime the keys are updated.

Additional key management best practices include:

- Have key custodians acknowledge their role and responsibilities by signing the attached Key Custodian Form.
- Restrict access to and the ability to change keys and passphrases for data encryption to the fewest number of custodians necessary.
- Store keys and passphrases (and backups of keys) in the fewest possible locations.
- Immediately change keys that have; reached the end of their crypto period, had their integrity weakened, have been or are suspected of compromise.

Computer and Network Security

Computer Security

To ensure that cardholder data is protected, it is important that appropriate security is enabled on all computers with access to the ChargeItPro software or data backups that include transaction information.

“Appropriate security” means, at a minimum, that:

- Default login names and passwords are immediately changed after installation.
- Each user is assigned a unique login name and password.
- Operating system updates, especially security patches, are applied on a regular basis.
- Virus protection software is installed and updated daily.
- The security risk introduced by other software installed on the same computer as ChargeItPro is evaluated and software that is not essential or presents a significant risk (such as remote access software) is removed.
- Limiting the use of file and directory sharing is strongly encouraged.
- If users have non-console access to the ChargeItPro Server, the use of SSH, VPN or SSL/TLS for encryption is strongly recommended.

Network Security

ChargeItPro must be installed in a protected network environment.

This means that:

- ChargeItPro should never be installed on a web server, ftp server or any Internet-accessible system.
- All computers with access to ChargeItPro should be behind a properly configured firewall with NAT enabled. Inbound access should be limited to essential services and the security ramifications should be clearly understood.
- Personal firewall software should be installed on any mobile or employee-owned computer with direct connectivity to the Internet, if those devices are used to access the organization’s network.
- If a wireless network is used, a perimeter firewall should be deployed to control or deny access to from the wireless network to the payment card environment.
- Passwords for DSL or cable modems, routers and firewalls, and all other internet hardware, should be changed to comply with the password recommendations

outlined earlier (complex passwords). Remote access to these devices should be removed and should only be used on an as-needed basis for a specific support requirement.

Note: Transmission Across Public Networks

All transmission of cardholder data across public networks must be encrypted. ChargeItPro does not support the use of email or end-user messaging (IM) for the transmission of cardholder data.

Use of Wireless Networks

ChargeItPro 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.

If you choose to deploy a wireless network infrastructure to support communications between deployed systems, or you connect a wireless network to the environment supporting the ChargeItPro application, you must do so in a manner compliant with the current PCI SSC DSS standards. The secure deployment of a wireless network is solely your responsibility. In order for you to achieve PCI SSC 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 you have wireless network deployed within your environment and it is not part of your 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.

Remote Access to your Network

ChargeItPro is delivered with an outgoing remote access capability that meets the requirements of the PCI SSC DSS. Remote access can only be initiated by the end user and the end user remains in control of the remote session at all times.

Access to remote sessions by ChargeItPro technical personnel is strictly controlled, is password protected, and requires two factor authentications. All remote sessions are logged in detail and are regularly reviewed by ChargeItPro management. If another remote access solution is to be used, it must adhere to the current PA-DSS requirements for payment card applications.

The remote access software must provide for the following features or configuration settings:

- You 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 or 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: Remote Administrative Access

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.

Data Retention and Transmission

ChargeItPro securely deletes sensitive cardholder data automatically upon completion of the authorization per DOD 5220.22-M guidelines. By default, ChargeItPro deletes protected cardholder data whenever a transaction batch is settled. If you wish to retain protected data, you may modify this setting in the ChargeItPro Server Setup. You should only retain protected data if there is a specific, identifiable need. If data is retained for any period of time and/or you are backing up this data, you should develop a plan to ensure that both the protected data and the backups are securely deleted when they are no longer needed.

Any cardholder data exceeding the customers defined retention period must be purged based upon business, legal, and/or regulatory requirements. When ChargeItPro is set to retain protected data past a transaction's authorization it is stored in the *Account_Number* field of the *History* table within the ChargeItPro database and is automatically purged using DOD 5220.22-M guidelines at the end of the retention period defined in the ChargeItPro Server setup.

Note: Retention of sensitive data in previous ChargeItPro releases

The previous releases of ChargeItPro reference the retention of 'Sensitive' cardholder data. This data is now referred to as 'Protected' cardholder data. ChargeItPro has never retained the data defined in this document revision as sensitive (magnetic stripe data, card verification values or codes, or PINs/PIN block data).

Data Backups

By default, ChargeItPro performs a daily backup of the program and data files to a backup folder in the ChargeItPro root directory. This backup may not be sufficient to recover data after a hardware failure as it resides on the same computer as ChargeItPro.

You may elect to perform a second backup of the data and program files by selecting this option in ChargeItPro Server Setup and setting the appropriate path for the second backup. It is strongly recommended that you not back up the data files to the same location as the program files in the secondary backup. Ideally, this backup should also be made to a different network drive than the automatic backup (or to removable media). It is critically important that you properly secure these backups as they may contain "Protected" cardholder data.

Control of Protected Data Used in Support Activities

In the process of supporting ChargeItPro, it may be necessary to collect customer data, including protected data, to resolve a specific technical issue. Protected data includes: the primary account number (PAN).

To ensure compliance, ChargeItPro technical support and merchants should adhere to the following:

- Only perform the collection of protected authentication data when needed to solve a specific problem.
- Collected data should be stored in a specific, known location with limited access; do not store the data on a web server or an FTP server.
- Only collect the minimum data needed to solve the specific problem.
- All collected data must be encrypted when stored. We suggest storing the data on an encrypted volume that is protected by a strong password. Software such as TruCrypt™, or similar, may be used to create an encrypted volume.
- Collected data must be securely deleted immediately after use. The data is to be securely deleted using tools which utilize the DoD 5220.22-M (7-pass) military grade secure deletion process. Software such as Eraser™, or similar, can be used to securely delete data in compliance with this DoD (Department of Defense) standard.
- Sensitive authentication data (magnetic stripe data, card validation codes or values, and PINs or PIN block data) must not be collected for any reason by ChargeItPro Staff even upon request by the customer or merchant.

FTPS Log Transmission

To assist in resolving a technical issue or to monitor your initial installation, ChargeItPro technical support may request your permission to transmit detailed transaction logs to a secure ChargeItPro FTPS Server. These logs contain no sensitive cardholder data.

Access to these logs by ChargeItPro personnel is strictly controlled and is password protected. Transmission of your logs via FTPS will only be undertaken with your permission and only for the amount of time required to resolve the technical issue or monitor your installation. All logs are securely deleted when no longer required.

Third-Party Integration

ChargeItPro can be used as a standalone application or it can be integrated with other third-party software. In standalone mode, all communication between the ChargeItPro client and server is routed though secure socket communication (SSL). In integrated mode, ChargeItPro supports both a file based and a socket based system for communication between the third-party application and the ChargeItPro server.

The file based system is provided for backward compatibility and is not PA-DSS compliant as it requires shared directories and a request and answer file communication format. Since Version 1.1 Build 337, ChargeItPro securely wipes all request files it processes and secures all transmissions between the ChargeItPro server and the Processor.

With ChargeItPro version 4.0 Build 803 file based system support is eliminated.

The secure socket based system is implemented through the use of the ChargeItPro EasyIntegrator™, which is available in a .Net DLL or an OCX component for Win32 applications. We encourage third party integrators to utilize EasyIntegrator™ to ensure a highly secure integrated environment for payment processing.

Software Upgrades

Upgrading or Replacing Card Processing Software

When upgrading from any version of the ChargeItPro software or when replacing other credit card processing software, it is essential that the previous application, backup files, cryptographic keys and other sensitive data be securely deleted by using a wipe tool, such as Eraser™, as described in the section titled *Control of Sensitive Data Used in Support Activities*. In addition, all unused areas on the disk should also be wiped. Such removal is absolutely necessary for PCI DSS compliance.

ChargeItPro Security Update Process

In the event that a security update is required, ChargeItPro will notify all customers by e-mail of the need to upgrade. Software updates will be transmitted to each customer's site with complete instructions for installing the updates.

Technical support will be available to assist customers in the upgrade process, if necessary. If updates are downloaded via the Internet, a personal firewall product should be installed to secure these "always on" connections.

Industry Resources

The links provided below for industry organizations and third-party security products mentioned in this guide were current as of the publication date. Payment Processing Partners does not own, control, or endorse the organizations or products listed.

PCI Securities Standards Council

Access industry information or download the PCI DSS standard and related documents.

https://www.pcisecuritystandards.org/

PCI SSC Self-Assessment Questionnaire

Access and use a self-assessment questionnaire as a tool to validate compliance with the PCI DSS.

https://www.pcisecuritystandards.org/saq/index.shtml

Payment Application Data Security Standard (PA-DSS; formerly Visa PABP)

Download a copy of the current requirements and assessment criteria for card payment software applications.

https://www.pcisecuritystandards.org/pdfs/pci_pa_dss.pdf

TrueCrypt™ Encryption Software

www.truecrypt.org/

Eraser™ Secure Deletion Utility

http://www.heidi.ie/eraser/

Revision History

The revision history 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 and itemized list of changes to this guide:

Document Version #	Description of Change
1.22	Initial revision tracking started; Updated URL link to PCI SAQ; Updated URL link to PA DSS Requirements
1.23	Updated card brand logos; Updated select payments industry terminology
4.0	Updated for PCI v2.0 Updated for ChargeItPro release 4.0

Updates to this guide are available through the ChargeItPro support site for registered customers. All ChargeItPro 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: **800-989-2135**.

Appendix A – Sample Key Custodian Form

All Company staff that hold responsible authorized positions where they manage or handle encryption keys must sign the following document.

As a condition of continued employment with Company, and as an employee that has access to key management tools and equipment, you are obligated to sign the following to indicate acceptance of your responsibility.

The signatory of this document is in full employment with Company on the date shown below and has been afforded access to key management devices, software and equipment, and hereby agrees that, he or she

1. Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of his/her ability, and has been trained in security awareness and has had the ability to raise questions and has had those questions answered satisfactory;

2. Understands that non-compliance with the key management procedures can lead to disciplinary action including termination and prosecution. Exceptions to compliance only occur where such compliance would violate local, state, or federal law, or where a senior officer of the company or law enforcement officer has given prior authorization;

3. Agrees to never divulge to any third party any key management or related security systems, passwords, processes, security hardware or secrets associated with the Company systems, unless authorized by an officer of the Company or required to do so by law enforcement officers; and

4. Agrees to report promptly and in full to the correct personnel, any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.

I agree to the above and understand that this original copy will be held on my personnel record and kept by the company indefinitely.

Signed:

Print Name:

Date: