POSitive products and PCI compliance

If you accept credit card payments in your business, you are required to comply with the Payment Card Industry (PCI) Data Security Standard. This standard has been adopted by most major card brands, including Visa, MasterCard, American Express, Diners Club, Discover Network, and JCB. It sets out twelve requirements that merchants must meet in order to protect cardholder information.

In this document, we'll discuss ways that POSitive products can help your business comply with the PCI standard, and set out some specific responsibilities that business owners must meet in order to make a POSitive system compliant with the standard.

This document is not intended to replace or stand in place of the PCI Data Security Standard and should not be exclusively relied upon to comply with the standard or with other requirements set out by your bank. POSitive strongly recommends reviewing the full text of the PCI Data Security Standard, available at https://www.pcisecuritystandards.org/ .

We also strongly recommend installing POSitive products into a secure environment, according to the recommendations in this document. Keep in mind that the use of POSitive products alone is not enough to comply with the PCI Data Security Standard.

How POSitive Software Products helps with compliance

In order to help our users comply with the PCI Data Security Standard, and in order to pass the PCI audit, we have implemented the following features and security measures in our software:

- Full magnetic stripe or CVV2 data is not retained. POSitive products do not store sensitive authentication

- Cardholder information that was stored by previous releases of POSitive products is securely deleted wh
- Encryption keys can be replaced regularly, and old keys are not retained.
- POSitive software allows you to create a unique user account (employee ID and password) for each em
- POSitive software maintains event logs that record each time an employee logs on to the program, whe
- POSitive products can be implemented with confidence into a secure network environment. The progra
- POSitive POS products do not provide Internet access to stored cardholder data, and they do not requir
- POSitive POS products do not enable remote access.
- Transmissions of cardholder data over public networks and the Internet are encrypted using Secure Soc
- POSitive POS products do not allow unauthorized users to view card numbers or to send cardholder inf
-

Web-based or remote administration, including non-console administration, is not supported by POSitive

Updating to the current POSitive release

There have been several changes in the most recent update of POSitive Products in order to meet PCI requirements. They are:

- Passwords are required when adding a new employee. If you have been adding employees without passwords, you should go and create passwords for each employee.

- The encryption key can now be changed. If you are storing credit cards (for recurring billing or for e-commerce processing) you should change your encryption key at least every six months.

Previous releases of POSitive products do not have these features, and you should update to the current release in order to meet your PCI requirements as regards software usage.

POSitive has two distinct classes of products; POSitive Retail Manager group, which includes POSitive GEM; and the POSitive For Windows group, which includes Averasell .

Updating POSitive Retail Manager/POSitive GEM

You can download the latest update from www.gopositive.com.

Before installing the update, you should make sure that you have closed any open credit card batch, and then backup all of your data. Also, if you have received any e-commerce orders that you have not processed the credit card deposit for, you should do that before updating as well.

Use Microsoft SQL Management Studio Express (or similar) to backup your SQL data. In addition, we recommend creating a new folder called POSBACKUP and copying the entire POSitive folder (PRM or GEM folder) into it. After the next routines are run, this backup and the backup folder should be deleted.

Once you have done your backups, you need to update and run PRM/GEM.

The update routines are launched when you first run PRM/GEM after the update. You will be stopped at a Security Update screen which has one option, which is "I do not store credit cards; remove all stored Credit Card information". This should be checked ON before clicking the "Process" button if you do not store credit cards for recurring billing or for e-commerce processing, and you do not store customer credit card information for any reason. If you are a "Cash and Carry" type of store, and you simply swipe cards and batch out at the end of the day, then you should check this option. This will remove any credit card information that may have been previously stored in POSitive, and allow you to answer the short questionnaire when performing your PCI Compliance self-evaluation.

Once you have decided whether you store credit card information or not, click the "Process" button. This will perform the necessary maintenance routines as required to comply with the PCI guidelines.

PRM/GEM will then launch as normal. If you are storing card information, you should check to make sure the maintenance routines have performed correctly. If you have recurring invoices, check your recurring settings to make sure the cards display properly. If you store credit cards in the customer table, make sure these are displaying correctly.

Finally, you should change your encryption password. There is a new security setting to allow changing of the Encryption key, so you will need to go to the Employee center and give yourself permission to change the encryption key. Then, go to Credit Card Manager, and select Change Encryption from the left-side menu. You will be prompted for your old encryption key, and your new encryption key. Click "Process". After the Process is done, again check your recurring settings and customer stored cards to make sure they display correctly.

Updating POSitive For Windows/Averasell

You can download the latest update from www.gopositive.com.

Before installing the update, you should make sure that you have closed any open credit card batch, and then backup all of your data. Also, if you have received any e-commerce orders that you have not processed the credit card deposit for, you should do that before updating as well.

You can use the internal backup routines in POSitive. In addition, we recommend creating a new folder called POSBACKUP and copying the entire POSitive folder (PFW folder or AVERASELL folder) into it. After the next routines are run, this backup and the backup folder should be deleted.

Once you have done your backups, you need to install the update. Once installed, navigate to the PFW/Averasell folder and run the CCCLEAR.EXE program. This program will remove any existing credit card data, or, if you are storing credit card information, make sure that it is stored correctly.

The update routines are launched when you first run PFW/Averasell after the update. You will be stopped at a Security Update screen which has one option, which is "I do not store credit cards; remove all stored Credit Card information". This should be checked ON before clicking the "Process" button if you do not store credit cards for recurring billing or for e-commerce processing, and you do not store customer credit card information for any reason. If you are a "Cash and Carry" type of store, and you simply swipe cards and batch out at the end of the day, then you should check this option. This will remove any credit card information that may have been previously stored in POSitive, and allow you to answer the short questionnaire when performing your PCI Compliance self-evaluation.

Once you have decided whether you store credit card information or not, click the "Process" button. This will perform the necessary maintenance routines as required to comply with the PCI guidelines.

Once this process is complete, exit CCCLEAR and run PFW/Averasell. If you are storing card information, you should check to make sure the maintenance routines have performed correctly. If you have recurring invoices, check your recurring settings to make sure the cards display properly. If you store credit cards in the customer table, make sure these are displaying correctly.

Finally, you should change your encryption password. There is a new security setting to allow changing of the Encryption key, so you will need to go to the Employee center and give yourself permission to change the encryption key. Then, go to Credit Card Manager and select Change Encryption from the button at the top right. You will be prompted for your old encryption key, and your new encryption key. Click "Process". After the Process is done, again check your recurring settings and customer stored cards to make sure they display correctly.

General recommendations

In this section, we'll provide some general recommendations for complying with the PCI Data Security Standard.

Important!

To ensure that you are fully compliant, read and implement the entire list of requirements in the PCI Data Security Standard. The standard includes very detailed and specific rules for merchants. It is available at https://www.pcisecuritystandards.org .

You should:

- If using PRM/GEM, you should disable or prohibit the use of the Microsoft SQL Server account "sa". If you leave the account enabled, ba SQL Server 2005 Security Best Practices

- Direct cashiers to log on to Windows using an account that does *not* have administrator access. For more information, searc

- Control access to all versions of POSitive and your store data by assigning a unique employee ID and p

- If you are using Microsoft Windows XP, turn off System Restore. The restore points saved by this featur Knowledge Base article 310405

- Perform regular audits and spot-checks of employee activities and program access.

- Periodically reset the encryption key for the store database. You can re-set the key by accessing the Cre

- If you choose to use wireless connections make sure you are doing so in accordance with PCI requirem

- Refrain from storing cardholder data on servers or computers that are connected to the Internet.

Note

The PCI Data Security Standard recommends the use of a dedicated database computer.

Requirement-by-requirement recommendations

In this section, we'll provide some specific recommendations for complying with each of the requirements of the PCI Data Security Standard.

Build and Maintain a Secure Network

(1)

Install and maintain a firewall configuration to protect cardholder data

In addition to hundreds of available security and policy settings, Microsoft Windows XP Service Pack 2,

(2)

Do not use vendor-supplied defaults for system passwords and other security parameters

After logging in the first time, secure the default user account in POSitive POS products. You can create

Protect Cardholder Data

(3)

Protect stored cardholder data

In addition to the masking and encryption in the store database, you can use the Encrypting File System

Windows Vista Enterprise and Ultimate editions include BitLocker Drive Encryption, a data protection featur
Windows Vista Features Explained - BitLocker Drive Encryption
Encryption .

(4)

Encrypt transmission of cardholder data across open, public networks

As mentioned earlier, POSitive POS encrypts all cardholder data and uses 128-bit-encrypted SSL transm

Encryption keys from previous releases of POSitive POS are securely encrypted and stored in a separat

Maintain a Vulnerability Management Program

5

Use and regularly update anti-virus software

Windows Firewall is a primary defense against viruses, worms, and the like. Additional security should b

6

Develop and maintain secure systems and applications

Use Microsoft Update to receive the latest security patches and software updates for Microsoft software.

Implement Strong Access Control Measures

7

Restrict access to cardholder data by business need-to-know

In Control Panel, use User Accounts to manage user profiles and access. In Windows Explorer, set perm

You can also set up security—employee by employee—for many of the features in POSitive POS.

8

Assign a unique ID to each person with computer access

See "General recommendations" earlier in this document.

You can use a screen saver that requires entry of a password to meet the idle terminal requirement of su

9

Restrict physical access to cardholder data

For some tips for making your physical location more secure, see these articles on www.microsoft.com:

- 5-Minute Security Advisor - Basic Physical Security
- Tighten in-house security
- 22 Questions That Can Help Protect Your Business

Regularly Test and Monitor Networks

10

Track and monitor all access to network resources and cardholder data

The Windows Firewall security log is a record of successful connections that go through the firewall and

11

Regularly test security systems and processes

Windows Firewall and Windows Defender can help you protect your system and detect threats. Both too

Windows Live OneCare offers anti-virus, spyware, and online ID protection, in addition to providing a firew

Internet Protocol Security (IPSec) is a key line of defense against internal, private network, and external

Maintain an Information Security Policy

12

Maintain a policy that addresses information security

As a supplement to the security policy that you develop to comply with this requirement, you can set up