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.

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 current security best practices. Keep in mind that the use of POSitive products alone is not enough to comply with the PCI Data Security Standard. Consult with your dealer or IT professional if you need assistance.

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 authentic
- Cardholder information that was stored by previous releases of POSitive products is securely delete

- 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
- POSitive software maintains event logs that record each time an employee logs on to the program,
- POSitive products can be implemented with confidence into a secure network environment. The pro
- POSitive POS products do not provide Internet access to stored cardholder data, and they do not re
- POSitive POS products do not enable remote access.
- Transmissions of cardholder data over public networks and the Internet are encrypted using Secure
- POSitive POS products do not allow unauthorized users to view card numbers or to send cardholde
- Web-based or remote administration, including non-console administration, is not supported by POS

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:

- You should disable or prohibit the use of the Microsoft SQL Server "sa" account when ac
- Direct cashiers to log on to Windows using an account that does not have administrative access. For more information, searc
- Control access to all versions of POSitive and your store data by assigning a unique employee ID a
- 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
-

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

-

Refrain from storing cardholder data in plain text on servers or computers that are connected to the

Note

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