

PCI Self-Certification Support Documentation
Combined Online and Kiosk - CardConnect

The Payment Card Industry Data Security Standard (PCI DSS) was created by the major card brands to establish security standards and specific measures that merchants must take to protect cardholder data and minimize the risk of a security breach. Anyone who accepts credit/debit cards directly or indirectly falls under these requirements. SecureGive and our partner gateways and processors are all PCI compliant leaving only a small amount of the responsibility to you.

To complete your compliance: Go to <https://cardpointe.managepci.com/safemaker/login/portal>.

You should have received a username and a temporary password from

CardPointe.com when your merchant account was first opened. If you do not have these or you need a reset, you can contact us.

Disclaimer:

The information contained in this document is not suitable for every organization. Each organization should answer the questions presented in the self certification process as honestly and accurately as possible. This document may be used as a reference that indicates a compliant response for some scenarios, but selecting a compliant response does not guarantee your actual compliance. This document is provided as a guideline only. If you have questions during the self certification process, you can reach out to VikingCloud/SecureTrust at 1-877-257-0239 or SecureGive at 855-895-8951 or support@securegive.com

Please note the following recommendations:

- *You should not be allowing donors to write down card information
- *You should have a privacy policy in place for all staff coming into contact with donor information.
- *You must now scan your internet network as well as your website if it contains a link to Securegive. If there is a link to SecureGive on your website, you must monitor to make sure that no one has tampered with that link.
- *There is no electronic storage of card data on your part.
- *We do not recommend admins sharing logins.
- *We recommend that admins change their password every 90 days
- *Be sure to delete admin access immediately following the departure of any employee.

There are now three sections to the Compliance process: Your Business Profile, Security Assessment, and Scan Compliance. Be sure to complete all three.

YOUR BUSINESS PROFILE:

*Please read PCI DSS 4.0 Update: **Check I understand and Next**

*Choose an Assessment Method: **Choose Expert and click Next**

***Self Assessment Questionnaire (SAQ) D**

*Does your compliance assessment require Scanning? **Click Yes**

*Third Party Payment Service Providers: **Answer Yes**

*Your outsourced third party payment service providers:

Select the following:

Payment processor or gateway

Virtual Terminal provider

Web hosting or co-location provider

Mobile Application provider - if you use our mobile app.

*Please provide the name of your e-commerce web hosting provider:

Type in Securegive. There will be no results found and you will need to click Add Your Own.

*Your Payment Gateway/Processor:

For the Monetra gateway, Type in/Choose Main Street Softworks then also CardConnect.

For the CardConnect gateway, Type in/Choose only CardConnect

***Contact us if you are unsure of your gateway.**

*Your Mobile Payment Application:

Type in SecureGive

*Your Virtual Terminal Provider:

Type in SecureGive. There will be no results found and you will need to click Add Your Own.

*Password Policy:

Answer Yes

*Do you use an Internet Security Assessor for your PCI DSS?

Answer No unless you have employed one.

*Support from a PCI Qualified Security Assessor

Answer No unless you have employed one.

*Third Party Managed System Service Providers

Answer Yes

*Managed System Component Providers:

Enter SecureGive and whoever hosts your website if SecureGive is connected to it.

*Other Third Party Service Providers:

Answer No

*A Summary of How and Where You Handle Card Payments:

Type this in all three blanks:

We are a church that receives donations through a link on our website that directs donors to third party PCI compliant Service Providers to take card info and process transactions. Card data is never entered into our website. We also have a donation kiosk with an encrypted card reader that connects to a third party PCI compliant Service Provider to process the donation.

If you use our mobile app, you can add this as well: **Donors can also access the donation system through a mobile app provided by SecureGive.**

COMPLETE SECURITY ASSESSMENT:

Click Manage and Answer Now to begin.

Requirement 1 : Answer Yes to all except:

1.4.4 N/A - No system components store cardholder data

1.5.1 N/A - No devices connected to CDE

Requirement 2: Answer Yes to all except:

2.2.5 N/A - No insecure services, protocols, or daemons present

2.3.1 and 2.3.2 - You must answer this for your organization. If using a kiosk connected to Wi-Fi, encrypted/tokenized data is being sent through your wireless network.

Requirement 3: Yes to all except:

Requirement 3.1.1 and 3.2.1: **You can answer N/A as long as you do not allow donors to write down card information. Then under the explanation, simply say “We do not store account data.”**

3.3.1- N/A - SAD is not stored electronically

3.4.1 - N/A - PAN is not stored or displayed - tokenization used.

3.5.1 - N/A -PAN not stored, tokenization used.

3.5.1.3 - N/A - disk level/partition level encryption not used. Tokenization used. PAN not stored

3.6.1 through 3.7.8 N/A - Tokenization used. No access to cryptographic keys.

Requirement 4:

4.1.1 and 4.1.2 Answer Yes

4.2.1 through 4.2.2 N/A - PAN is never transmitted. Tokenization used.

Requirement 5,6,7: Answer Yes to All

Requirement 8: Yes to all except:

8.4.1 N/A - No access to CDE

Requirement 9: Yes to all except:

9.2.1 and 9.2.1.1 - N/A - NO physical access to CDE

9.2.2 - N/A - No physical access to facility

9.2.3 - You must answer for your Wi-Fi if you have a kiosk connected to it.

9.3.1 through 9.3.4 - N/A - No physical access to CDE

9.4.1 through 9.4.5.1 - N/A - No media with cardholder data

9.4.6 N/A unless you allow donors to write their card number down.

9.4.7 - N/A - No media with cardholder data

9.5.1 through 9.5.1.3 You are responsible for completing these items in relation to kiosks.

Requirement 10: Yes to all except:

10.2.1.1 N/A - No access to CDE

Requirement 11: Yes to all except:

11.2.1 through 11.3.2.1 - You are responsible for these items as it relates to your kiosks - Monitoring kiosk environment, Wi-Fi connections, completing scans of network. You must also now scan your website if SecurGive is embedded or linked to it.

Requirement 12:

In order to answer Yes to these, you must make sure you are maintaining a list of third party service providers that you contract with and you are making sure they are PCI compliant. This would include SecureGive and your merchant processor. When asked for a date, you can put the date of completing your questionnaire. You should also make sure that you have an incident response plan in the event that you suspect a breach. (As long as you are not allowing donors to write down card numbers and you are making sure your website is monitored and secure, then the only other thing would be to contact us if you suspect a breach.) You should also have a security policy in place in relation to monitoring kiosks, and your internet network.

This should bring you to the screen to Confirm your Compliance by entering your **Organization Information Details, then Merchant Executive Officer Details and Confirm your Attestation.**

BE SCAN COMPLIANT

Your final step will be to schedule a scan of your website (if SecureGive is embedded or linked) and of the IP address that your kiosks are connected to. Do not use the IP address that pulls up automatically on your screen. It is pulling from whatever internet network that your device is connected to. You would enter your website address and also check the IP address that your kiosks are connected to by going to the kiosk itself. Open a web browser on the kiosk and access the internet. Then type in "What is my ip address?". Use the number that comes up. You will get results within a day or two and will need to sign in and attest to your results or address any issues found.

*You will not be compliant until you attest to the results.

When signing back in to attest to passing results:

1. Go to <https://cardpointe.managepci.com/safemaker/login/portal> and sign in.
2. Under Be Scan Compliant, Click Manage
3. Review your PCI DSS External Vulnerability Scans
4. Click Options then Attest - * If Attest is not showing, you may still need to just answer some questions before you can attest. To do that:
5. Click Options and Review on the Passing Scan
6. Click on Related Hosts - Answer No to all
7. Click on Special Notes and Click Declaration and answer Yes, then Submit
8. Once you have done that, if it doesn't automatically take you to a screen to Attest, you can get to it by going back to Review Scans, then Options should have Attest under it.

When signing back in to address any failing results on the scan:

1. Go to <https://cardpointe.managepci.com/safemaker/login/portal> and sign in.
2. Under Be Scan Compliant, Click Manage
3. Review your PCI DSS External Vulnerability Scans
4. Click Options then Review to see things that need to be Addressed. You can also Download the full report.

5. You will land on the Status screen with the overview
6. The Domains tab will let you see what website or IP address was scanned.
7. Under Related Hosts, you should be able to answer Not in Scope to any they found.
8. Under Scan Vulnerabilities, filter by PCI Compliant: No to see what needs to be addressed
9. Under Each Vulnerability listed, you can click Show More to view the details and the solutions. These details can also be found on the full scan report. You would need to take this report of vulnerabilities and the solutions to whoever manages your website (if relating to your website) or to whoever manages your internet network (if relating to that IP address) to get their help in resolving them.
10. The Special Notes section may also contain some statements which need to be addressed. You would consult your website or internet manager on how to answer these as well then click on Declaration and note it there.

We definitely understand that this can be very confusing and frustrating. While we are doing our best to maintain PCI protections, we are also doing our best to help guide you through what may fall under your responsibility. We also know that you want to do everything within your power to protect your donors.