PCI Self-Certification Support Documentation
Kiosk only - 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) C**

*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
Any other third party provider…

*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.**

*Password Policy:
Answer **Yes**

*Third Party Managed System Service Providers
Answer **Yes**

*Managed System Component Providers:
Enter SecureGive

***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 donation kiosk with an encrypted card reader that connects to a third party PCI compliant Service Provider to process the donation.

<u>COMPLETE SECURITY ASSESSMENT:</u>

Click Manage and Answer Now to begin.

<u>#1 Questions</u> :
To answer Yes to these, you must make sure that the internet network connected to the kiosk is secure. The recommended protocol is to have the kiosk segmented from the rest of the network - not to have it connected to a Wi-Fi that others are accessing as well. NSCs are referring to Network Security Controls.

<u>#2 Questions</u>:
SecureGive has all of these In Place but you must also make sure you are adhering to them as it relates to the internet network connected to the kiosk.

<u>#3 and 4 Questions:</u>
Yes to all

#5 Questions:
SecureGive adheres to all of these. However, it is recommended that you use Malware especially if you use a Windows based kiosk and answer these questions accordingly.

#6 Questions:
Yes to all

#7 and 8 Questions:
SecureGive has all of these In Place. However, in order to answer Yes, you must also maintain a list of people with access to your SecureGive dashboard, merchant account, internet network controls, website administration, etc and make sure accesses are secure, kept up to date, and revoked when employees leave. Logins should not be shared.

#9 Questions:
Yes to all except listed below as long as you are restricting access to the internet network that the kiosk is connected to, you are monitoring the kiosk and inspecting regularly for tampering, and you are maintaining a list of the kiosk equipment.

9.4.1 through 9.4.6 N/A - No media with cardholder data present

#10 Questions:
Yes to all

#11 Questions:
You can answer yes to all as long as you know- You are responsible for these items as it relates to your kiosks - Monitoring kiosk environment, Wi-Fi connections, completing scans of network.

#12 Questions:
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. 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 monitoring your internet network and the kiosks, 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.

A2.1.1- N/A - SSL or Early TLS not used.

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 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 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 back in and attest to your Passing results or address any Failing issues found.

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 the internet network connected to the kiosks 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 IT person 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.