PCI Self-Certification Support Documentation
Online/Mobile 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.

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

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.

Please note the following recommendations:

*You should not be allowing donors to ever write down card information
*You should have a privacy policy in place for all staff coming into contact with donor information.
*You should be deleting admin access as soon as a staff member leaves your organization.
*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

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) A**

*Does your compliance assessment require Scanning? **Click Yes if you use a website in any way to direct to SecureGive.**

*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**

*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.
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.**

<u>COMPLETE SECURITY ASSESSMENT:</u>

Click Manage and Answer Now to begin.

Requirement 2.2.2: **Answer Yes**

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."**

Requirement 6.3.1 and 6.3.3**: Answer Yes**

Question Group 8: **SecureGive adheres to these policies but you must also make sure that anyone managing your website does as well if SecureGive is connected to your website to answer Yes.**

Question Group 9: **You can answer N/A to all of these as long as you do not handle actual card numbers (such as card numbers written down) at all. If you handle card numbers, you must evaluate the processes and answer these questions appropriately.**

Requirement 11.3.2.1 **You must begin scanning your website if it contains a link directing to SecureGive or if it has an embedded frame. You can answer Yes to that as long as you begin doing this and make sure it is scanned after any significant changes to the site.**

Question Group 12: **You should answer Yes to these and 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.)**

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. Under BE SCAN COMPLIANT, Click Manage. Then click Schedule Scan. Do not use the IP address that pulls up automatically on that screen. It is pulling from whatever internet network that your device is connected to. Enter your website address and schedule the scan. The answer should be No on Load Balancers. You will need to check the box at the bottom of the screen agreeing to the statement. 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 your website 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 host/provider on how to answer these then click on Declaration and note it there.

*After resolving scan vulnerabilities, you must rescan until you get a passing one.

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. Since SecureGive will be connected to your website, there is always a chance that someone could hack your website and mess with that link, counterfeit your website, or any number of things. That is why PCI regulations are now calling for scanning of websites with redirection URLs or embedded frames where transactions will be entered.