PCI DSS PCI Self-Certification Support Documentation
Combined Online and Kiosk - Fortis

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 Fortis at 1-866-377-3287 or SecureGive at 855-895-8951

To complete your compliance: Go to **https://pciapply.com/epic**
Your username is usually your primary merchant account number. If you are not sure of your login info or you need a password reset, you can contact us.

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.
*You must monitor your kiosks regularly to be sure they have not been tampered with.
*We strongly discourage having kiosks connected to a Wi-Fi that is also used by others.
*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.

Under Merchant Information:

Part 1 Merchant Information

Is your organization a service provider as defined by the PCI Council (e.g., hosting providers, payment processors, managed service providers)? **You will answer NO**

Part 2 Merchant Business Payment Channels
*__Choose E-Commerce and Card Present and answer NO to electronically storing or transmitting consumer account data.__

*Are any payment channels not included in this assessment? **You can answer NO** unless you have other means of donations or payments other than SecureGive.

Part 3 Relationships

*Do you have relationships with third party service providers that handle your account data such as payment gateways or processors? **Answer YES**
*Do you engage with third party service providers managing system components within your PCI DSS assessment scope? **Answer NO** unless you use web hosting services or network security, anti-malware services relating to the donation environment.
*Do you work with third party service providers that could impact the security of your cardholder data environment? **Answer YES**.
List the following:
Main Street Softworks Monetra - Payment Gateway
FortisPay - Merchant Processor
SecureGive - SaaS

Part 4 Processing Solution

Choose Moto/ECommerce if using our online giving
Choose Mobile Processing if using our mobile app
Choose Stand Alone Computer if using our kiosks

*Do you store any sensitive cardholder data electronically? **Answer NO**
*Does your business use network segmentation to affect the scope of your PCI DSS environment? Answer No unless you have your internet network segmented to separate the kiosk environment - then answer Yes.

*For Moto/ECommerce

How do you process payments? **Choose Hosted Payment/iFrame**

*Does your website use either a redirection mechanism or an embedded payment form? Answer **Yes**
***98.5% of merchants are susceptible to script attacks. Do you have in place monitoring for your payment page scripts to protect against such attacks? Answer **Yes**
***Describe how your site is protected from script attacks. Include details such as monitoring tools, security controls, or third-party protections in place. Enter this in the blank: **ReCaptcha, AVS and CVV verifications, Monitoring/Blacklisting IP addresses, Throttling, Velocity Checks, Monitoring Processing Patterns**

*Please add your Moto/ECommerce Solution Information:
Click Add Solutions.
Click on the blue line to add it manually
Service Provider: Monetra Service: Main Street Softworks

*For Mobile Processing, Choose **Cellular**
Click to Add Solutions
Click the blue line to add it manually and **type SecureGive in both blanks**.

*For Stand Alone Computer
Do you only process cards by accessing a payment website and typing in the card number?

Answer No
Then click to Add Solutions
Click the blue line to add it manually.
Vendor: **Monetra with Card Shield**
Application: **Main Street Softworks**
Version: **v9**

Check box that you have read and agreed to the end user license agreement
Click the Blue Box to Select the Questionnaire Manually.

Select Questionnaire D and Hit Continue

Software Selection:
Click the blue line to add manually and type **SecureGive** in the Vendor and Application blanks and **Multiple** in the Version
Does your business use network segmentation to affect the scope of your PCI DSS environment? Answer No unless you have your internet network segmented to separate the kiosk environment (If so, answer Yes).
Processing Solution: **Choose Multiple processing Solutions**
Provide a high level description…

"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.
Donors can also access the donation system through a mobile app provided by SecureGive."

Section 1
You can answer in place to all except #19. Mark as N/A and use the following explanation:
No computing devices connect directly to the CDE

Section 2
You can answer In Place to questions #1-5 then for #6 and #7 Mark as N/A and use the following explanation:
No insecure services , protocols, or daemons present.

For #10-11 - if you are using Wi-Fi for kiosks, you must answer for yourself. Encrypted card data is being sent through your internet connection.

Section 3
You can answer In Place to all except specific questions below:
#8 - N/A with explanation: No SAD stored electronically prior to completion of authorization
#10 - N/A with explanation: Not using remote access technology. No PAN stored. Tokenization used
#11, #13, #14 - N/A No PAN stored. Tokenization used
#15-26 - N/A with explanation: Tokenization used. No access to cryptographic keys.

Section 4
Answer In Place to all

Section 5

You can answer In Place to all except the following:
#10 - N/A - No removable electronic media

Section 6
You can answer In Place to all

Section 7
You can answer In Place to all

Section 8
Answer In Place except listed below:
#20, #21, #22 - N/A - No access to CDE
#24, #25 - N/A - No interactive login scripts

Section 9
Answer In Place for #1-2
#3 through #22 - N/A - No access to physical facilities or CDE. No media with cardholder data
#23-#27 - In order to answer In Place, you must monitor your kiosks and inspect regularly for tampering.
Section 10
Answer In Place to all except #4
#4 is N/A - No access to cardholder data

Section 11
You can answer In Place to all except #3, #4, #9, #10. You must make sure you are taking care of these in order to answer In Place. #7 is N/A - Not required until March 2025. No interactive login.
#18 - you must monitor your website and the redirection link attached to it if linked to SecureGive

Section 12
#7 is N/A - No cryptography used. Tokenization used.
#16 is N/A - No access to CDE
All other questions must be answered by you. Some of the items are not required until March 2025.

Section 13
Schedule your scans. If a link directs from your website to SecureGive online giving or you have an embedded frame, you must now scan
Your website as well as the IP address where your kiosks are located.
The most accurate way to find the IP address of your kiosk is to access the web browser on the kiosk (for example Google or Safari) and type in “What is my IP address?” A long number will come up on the screen. Use this to schedule the scan. You must have your scans run monthly but you are only required to have a passing scan on a quarterly basis. **Once you receive passing scan results, you must sign back into the PCI portal and submit them for ASV Compliance. If you do not complete this step, you will not be compliant.**

If your scans should fail, you will need to sign into the PCI portal and view the scan vulnerability reports to determine what may need to be addressed in order to pass the scans.