PCI DSS PCI Self-Certification Support Documentation
Online/ECommerce - 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.
*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 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

*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

***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**.

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 A and Hit Continue

Software Selection:
Click the blue line to **add manually** and type **SecureGive** in the Vendor and Application blanks

Does your business use network segmentation to affect the scope of your PCI DSS environment? **Answer No**

Under Moto/ECommerce, **Choose Hosted Payment and iFrame**

Does your website use either a redirection mechanism or an embedded payment form? **Answer Yes** if you have a SecureGive link attached to your website or you have SecureGive embedded into your website.

Confirm Your Eligibility to Complete Questionnaire A:
Agree to the statements and Continue.

Click Start Questionnaire at the bottom of the next screen.

Section 1
Question 1: Answer In Place
Section 2
You can answer In Place to questions #1-2 as long as you are not allowing donors to write down their card data for you to input donations for them. If you do that, you must have policies in place that govern retention and disposal of that information.

Section 3
You can answer In Place to all

Section 4
Answer In Place to all

Section 5
You can answer In Place to all as long as you are not allowing donors to write down card numbers. If you do that, you must have policies in place that govern storage, removal, etc.

Section 6
You can answer In Place to all

Section 7
You can answer In Place to all as long as you 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 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.)

Section 8
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

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.