PCI DSS PCI Self-Certification Support Documentation
Kiosk Only - 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 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 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 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 C 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 Stand Alone Computer via card scanner.**

Confirm your eligibility to complete questionnaire C:
Agree to the statements and hit Continue

Click Start Questionnaire at the bottom of the next screen.

Section 1

To answer In Place 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.

Section 2
SecureGive has all of these In Place but you must also make sure you are adhering to them as it relates to your kiosk - especially 1-4, 5, 9.

Section 3 and 4
You can Answer In Place to all

Section 5
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.
#9 - N/A - No removable electronic media
#12 - This is not required until next year so you can answer Not in Place with the explanation that you will put it in place by the deadline. This is referring to training staff against phishing scams.

Section 6
You can answer In Place to all

Section 7
SecureGive has all of these In Place. However, 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.

Section 8
Answer In Place except listed below:
Again, you must 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.
#22, #23 - N/A - No interactive login scripts
#14, #19, #21, #24 - Not in Place - Not required until 3/2025

Section 9
Answer In Place for #1
#2-4 In Place as long as you are restricting access to the internet network that the kiosk is connected to and you are monitoring the kiosk and inspecting regularly for tampering.
#5 through #10 - N/A - No media with cardholder data present.
#11-#14 is your responsibility relating to the physical kiosk.

Section 10
Answer In Place to all

Section 11

You can answer In Place to all as long as you are running your regular network scans. SecureGive does the others.

Section 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. 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.

Section 13

Schedule your scans. 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 Go to ASV Compliance Status, then view the scan vulnerability reports to determine what may need to be addressed in order to pass the scans.