What is CampusGuard?

CampusGuard is where merchants can complete their PCI (Payment Card Industry) required Self-Assessment Questionnaires (SAQ). With CampusGuard merchants are also able to store and review important documents related to their previous SAQ and PCI compliance.

The SAQ is designed as a self-validation tool to assess security for cardholder data. The SAQs are exact copies of those provided by the PCI Security Standards Council so you can rest assured you are responding to the correct requirements.

How do I gain access to CampusGuard?

Gaining access to CampusGuard can be done through emailing the UGA Credit Card Coordinator, Lauren Hofmann at hofmannl@uga.edu and include the merchant being added.

Logging in:

Once you have your login information, you will need to use the link https://portal.campusguard.com/login and you will be brought to the login page

Login with your User Name (typically your email address) and password. Upon login you will be redirected to your home page within the portal.

Portal Navigation

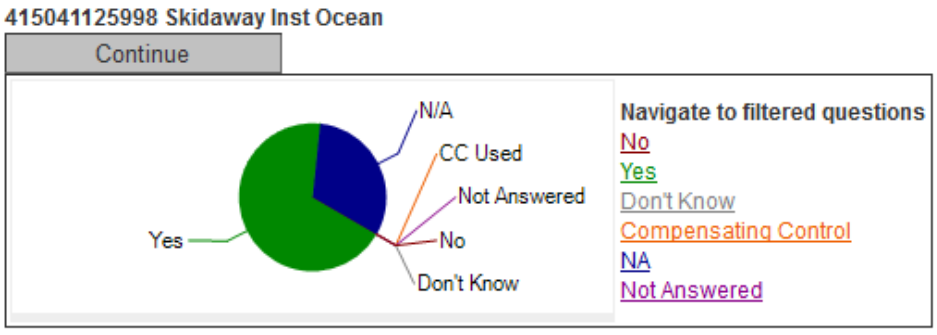
The top menu provides links to the different features within the Portal.

- **CampusGuard Home** – Direct link to the CampusGuard public website.
- **Portal Home** – Return to the User dashboard/home page on the portal.
- **Scanning Request** – Form used for requesting external vulnerability scans of your web applications or network resources.
- **Document Locker** – Secured folder that can be used to upload network drawings and/or documentation that support compliance objectives.
- **General Documents** – Read-only area used by CampusGuard to distribute common documents and resources to all users of the portal.
- **Help** – Create an email to the CampusGuard team or navigate to the PCI Council website.

User Dashboard

Users will have access only to the specific merchant or merchants they have been assigned. Upon login, please verify your assigned merchants look correct. To begin, you will select a SAQ or continue a SAQ in progress by clicking on the Start/Continue button located under the Merchant ID. This button will direct you to the first page of the selected SAQ.

From the User home page, you can also select to view a group of questions based on their response setting (Yes, No, Don't Know, N/A, Not Answered, and Compensating Control), by clicking on the respective hyperlinks in the pie chart that appears for each SAQ. For example, if you had previously attempted to complete your SAQ, but were uncertain on a number of requirements and had answered "Don't Know", you can now easily navigate to those questions by clicking on the gray Don't Know hyperlink.

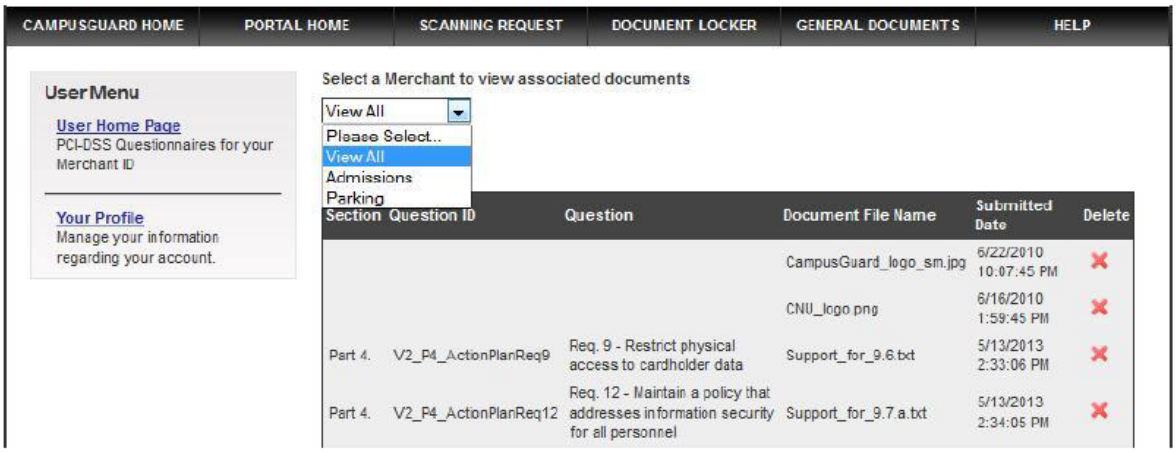


Self-Assessment Questionnaire B 3.2.1 and Attestation of Compliance, 3.21, Effective 5/1/2016 12:00:00 AM
Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals - No Electronic Cardholder Data Storage

Document Locker

The Document Locker is a secure location to store documents and network drawings to support answers given in the SAQ. The Document Locker is also used to deliver vulnerability scan reports from CampusGuard and store archived SAQs from previous years.

An example of a document that may be required is in SAQ D, Requirement 1, Question 1.1.2 which specifies a "current network diagram with all connections to cardholder data…" This drawing can be uploaded for future reference with this question. You may use any format for the document since the document will be stored in the same manner that it is uploaded. However for consistency, it is recommended that all documents be stored as PDF format. This will ensure that printing of the completed questionnaires and associated documents will function as expected.



Selecting the tab for the Document Locker from the Navigation bar reveals the above window. From here it is possible to:

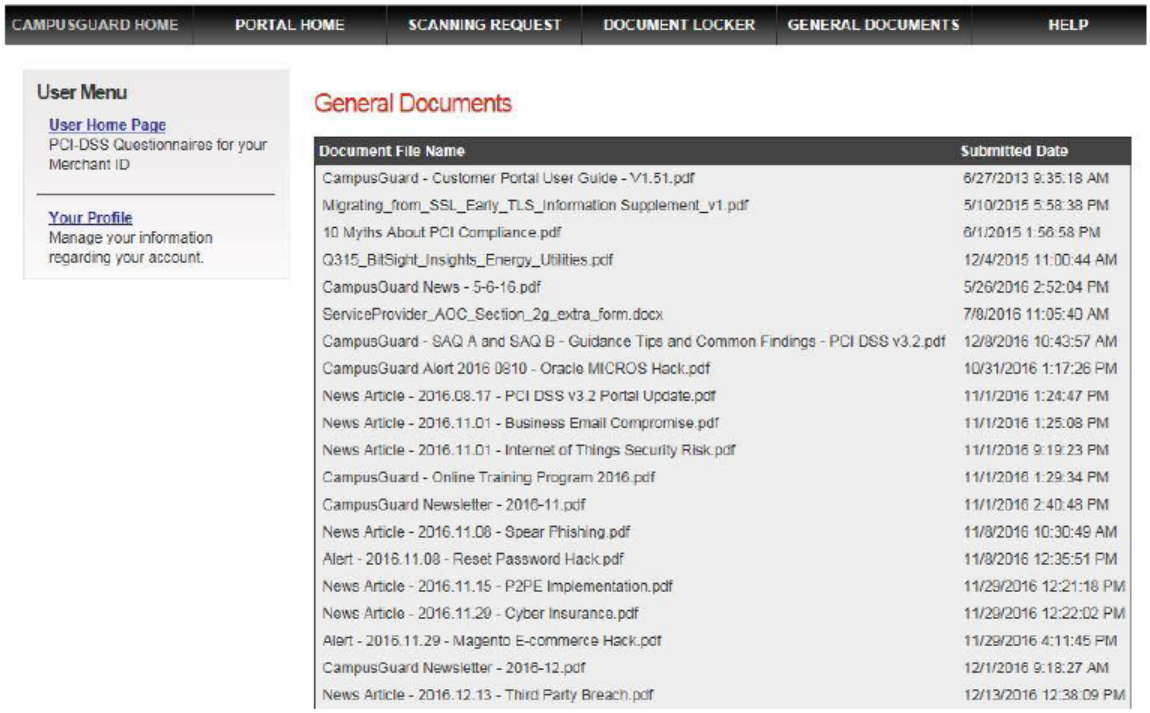
- Show all documents associated with a particular Merchant ID.
- Print archived documents, previous SAQs, and other documents.
- Upload additional documents.

To remove documents from the Document Locker, find the title of the document you wish to remove and then click the "X" in the Delete column. The document will be removed from the system.

***It is not possible to recover a document once it has been deleted, therefore be sure that is the action you wish to take.**

General Documents

The General Documents section of the portal contains documents that will be of use to all CampusGuard customers. This section is read-only for customers and you cannot upload documents here. CampusGuard reserves this area to distribute resources to the community, including news updates, alerts, guides, templates, and more. Selecting the General Documents tab on the navigation menu will reveal all items available for download. Click on the link of the document that you wish to obtain, and it will download to your computer in the location that you specify.



SAQ/Form Navigation

Clicking the Start/Continue button will generate the assigned questionnaire. The navigation frame will appear on the left replacing the User Menu. This frame provides statistical information about the SAQ / AOC.

Total sections – Number of sections within the SAQ.

Entry Requirements – Number of requirement questions to be answered.

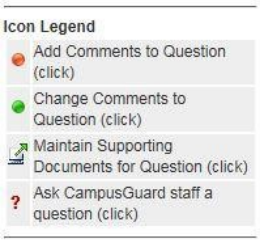
Entry Requirement Progress – A status bar showing the percentage of Requirements that have been answered. NOTE: the fields in Parts 1, 2, 3, and 4 are **not** included in this tally.

SAQ pages – Quick links to the specific pages of the SAQ / AOC.

Users may access any section and/or question at any time once they are within their selected SAQ / AOC. However, please remember to SAVE using the button at the bottom of each page before navigating away from a page.

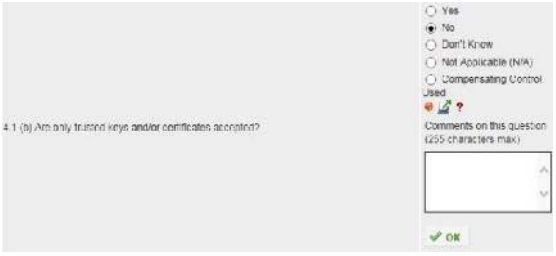
The Icon Legend and Helpful Tools

Throughout the SAQ, there are helpful tools to assist you in its completion. These tools are denoted by icons.



Add Comments

Clicking this icon generates a box to provide supplementary information regarding an answer to a requirement within the SAQ. You may add up to 255 characters of text to include additional details or clarification. It can also be used as a place holder to remind you to come back to this question. For example, you may just want to add a comment stating, "Need more information" so you can return to this question at a later time. Type your comment and click OK. All comments added in this box can be printed with the questionnaire.



Change Comments

If the comments icon is green, it indicates a comment has been saved for this question. Clicking this icon will allow you to review, edit, or delete the comment. You may add text up to 255 characters. Removing the text from this box and selecting "OK" will return the comments icon to red.

Upload Documents

This icon will generate a new window and allow you to browse your system files and upload a document associated with the requirement you are on. Although files of any type can be uploaded, it is recommended that all attached documents be saved in PDF format.

To use this feature:

- Select the icon on the specific question that pertains to the document being uploaded.
- Click the "Browse" button to navigate to the location on the users' system that the document resides.
- Select the document. □ Click "Upload File".

The document will then be uploaded and saved to the secure CampusGuard Document Locker. You can view uploaded documents by selecting the "Document Locker" Tab in the navigation menu**.**

Ask CampusGuard a Question

By clicking the question icon, a pop-up window will appear and allow you to generate a direct email to CampusGuard staff.

The email subject is auto-populated with the question number. Share your question or comments and click send. A CampusGuard team member will respond as quickly as possible. If you are confused and questioning what a specific requirement is asking or whether it applies to your environment, please do not hesitate to take advantage of this feature. Your Org Admin or PCI Team may also receive a copy of the question so they can provide assistance as needed.

The SAQ - Questionnaire

The primary function of the CampusGuard Compliance Portal is to facilitate the management of all merchant Self-Assessment Questionnaires (SAQs) for an institution. Specific SAQs are assigned to each merchant ID as required by the Acquirer (bank).

It is not necessary to complete the SAQ all at once. The SAQ can also be used as a working document to manage your journey towards compliance.

As a user you will only see those SAQs that have been assigned to you. To begin, select the gray Start button at the top left of the pie chart graphic.

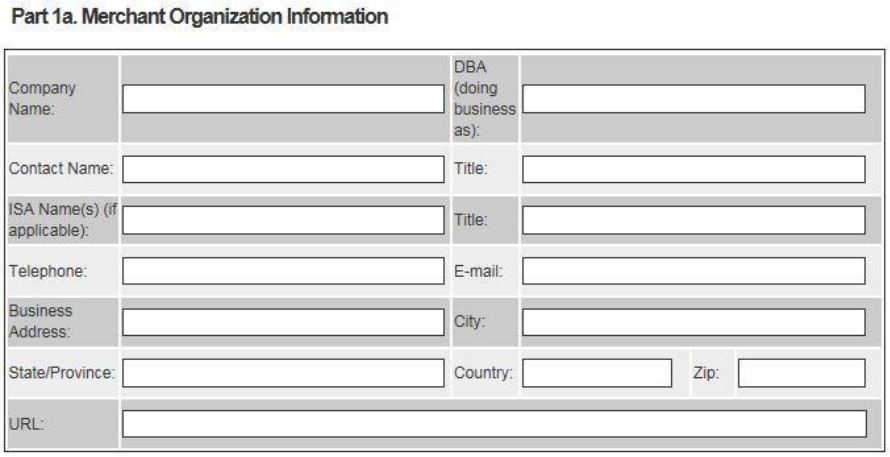
Be sure to save your work by clicking the Save/Next Page button at the bottom of each page. You can also print your SAQ by clicking on the Printable Version link at the top of the page.

Part 1 and Part 2

Part 1a. Merchant Organization Information

Complete this section with the contact information for the merchant area/department

- Company Name – Your institution's official name
- DBA(s) – Department that is using this Merchant ID Number (MID)
- Contact Information – Primary contact for this merchant



Part 1b. Qualified Security Assessor Company Information

Since you have contracted with CampusGuard for consulting services use the information in the image below to complete this section.

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Merchant Preservation Services, LLC d/b/a CampusGuard				
Lead QSA Contact Name:	enter your QSA's name	Title:	Security Advisor		
Telephone:	leave blank	E-mail:	leave blank		
Business Address:	8740 Lucent Blvd - Suite 440	City:	Highlands Ranch		
State/Province:	CO	Country:	USA	Zip:	80129
URL:	www.campusguard.com				

Part 2a. Type of merchant business

What type of payment channels does your business serve? Select the different payment channels that the merchant provides. Since the payment channels for college and university clients is widely varied, we suggest you do the following:

- Select "Others"
- For "Please Specify" type in **Higher Education**

Part 2a. Type of Merchant Business (check all that apply)

☐	Retailer	☐	Telecommunication	☐	Grocery and Supermarkets
☐	Petroleum	☐	E-Commerce	☐	Mail order/telephone order (MOTO)
? ☑	Others	(please specify):	Higher Education ?		

What types of payment channels does your business serve?		Which payment channels are covered by this SAQ?	
☐	Mail order/telephone order (MOTO)	☐	Mail order/telephone order (MOTO)
☐	E-Commerce	☐	E-Commerce
☐	Card-present (face-to-face)	☐	Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.*

Part 2b. Description of Payment Card Business

Enter in a short description of how this merchant stores, processes, or transmits cardholder data. Provide a high level overview of how cardholder data flows within your business and any third-party involvement. For example, "Customer visits our website, chooses a product to purchase, and is redirected to Authorize.Net for payment. The customer inputs their payment information, and the success or failure of the transaction is reported back to our server, along with a record of the item purchased and cardholder name." It is also useful to note "we do not store cardholder data at this time" or "we use PTS-approved swipe terminals" if applicable.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	

Part 2c. Locations

List the type of facility, number of facilities similar in structure and business process, and the locations of each facility. List only those locations that apply to this merchant. For example, the Dining Services SAQ may cover two types of outlets – on-campus dining halls and remote food cards. Each type would be listed on a separate line.

Part 2c. Locations

List types of facilities and a summary of locations included in the PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.)

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)

Part 2d. Payment Application

Does the merchant use one or more Payment Applications? A Payment Application is a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, and where the payment application is off-the-shelf software and is installed on the merchant's premises. PA-DSS does NOT include custom software created just for the merchant or software that is hosted by a PCI-validated third-party service provider that maintains the payment application. If yes, list the Application(s) being used for payment processing. Provide version number and application vendor.

The PCI SSC website can be used to determine whether a payment application is validated for use.

Part 2d. Payment Application

Does the organization use one or more Payment Applications?	○ Yes ○ No ○ Don't Know

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			○ Yes ○ No ○ Don't Know	
			○ Yes ○ No ○ Don't Know	
			○ Yes ○ No ○ Don't Know	

Part 2e. Description of Environment

Provide a high level description of the cardholder data environment (CDE). Include critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.

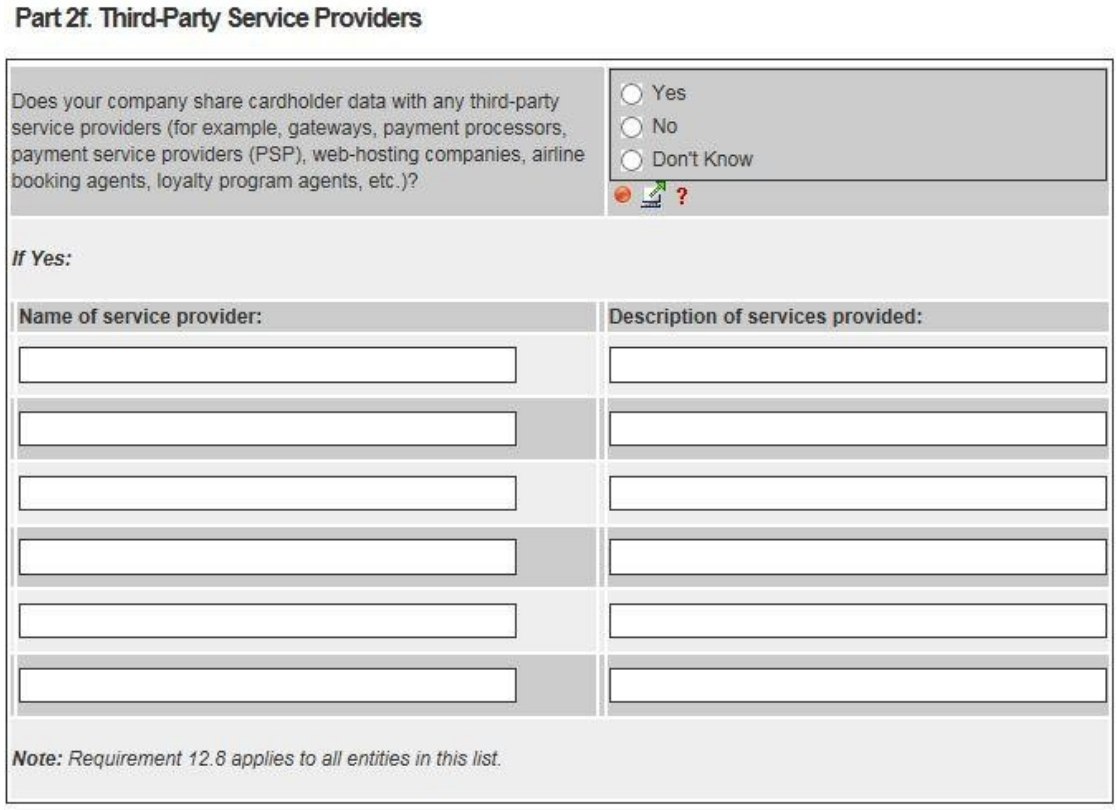
You will also be asked to indicate if your organization uses network segmentation to affect the scope of your PCI DSS environment. Network segmentation refers to the physical or logical separation between devices that handle cardholder data (CHD) and are in PCI scope from those that do not handle CHD and are not in scope for PCI compliance. If there are any additional firewalls, routers, virtual, or other systems in place that restrict network traffic to or from the systems within the merchant area (traffic that is otherwise allowed on the network), you would answer "Yes" to this question. If there are no systems in place that restrict traffic flows between the merchant area and the remainder of the campus network you would answer "No".

Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	○ Yes ○ No ○ Don't Know

Part 2f. Third-Party Service Providers

Third-party service providers are vendors that provide systems or services that store, process, or transmit cardholder data on the merchant's behalf, e.g. Authorize.NET, CyberSource, PayPal, etc., or are companies with whom CHD is shared for any purpose to support merchant payment processes. If cardholder data is shared with any third party, i.e. for payment processing or other services, you must answer "Yes" and provide the name of the vendor and the service they provide.



Part 2g. Eligibility to Complete AOC SAQ

All merchants MUST comply with the full PCI DSS, however, the various SAQs focus on specific payment channel requirements. The merchant must be able to indicate all statements listed here are accurate for their merchant area.

Part 2g. Eligibility to Complete AOC SAQ A-EP

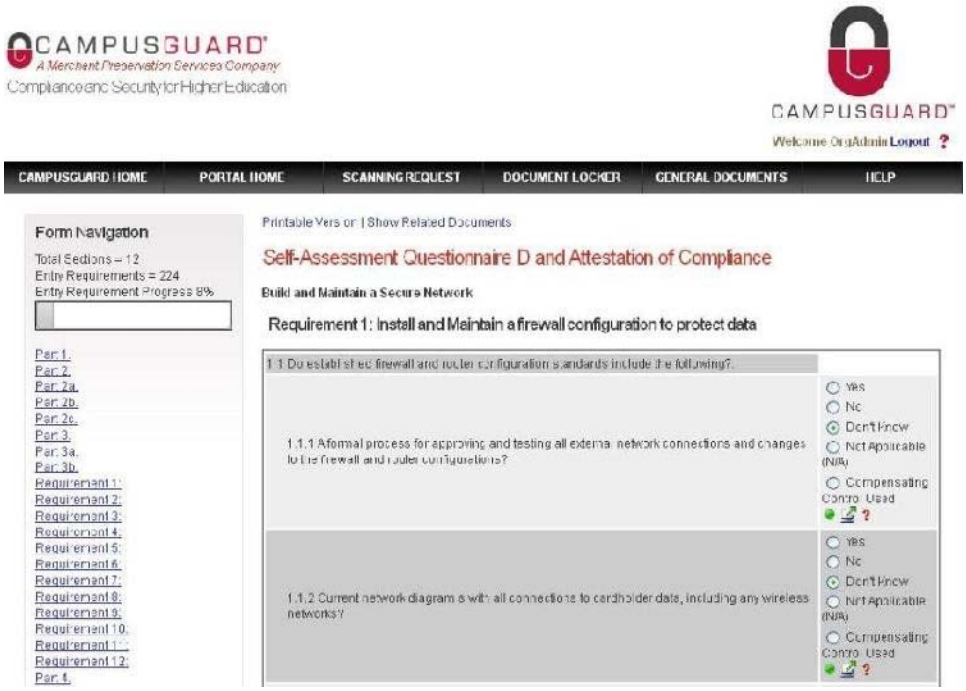
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

☑	Merchant accepts only e-commerce transactions;
☑	All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
☑	Merchant's e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
☑	If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
☑	Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
☑	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☑	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☑	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Requirements

This is the section of the SAQ that will vary depending on the questionnaire that you are answering. Since each questionnaire will address different parts of the PCI DSS and include differing questions, this guide will not detail how to answer each question. However, we encourage you to use the "**?**" to request help from the CampusGuard Team if you have questions or need assistance on a specific Requirement question.

Remember, to be fully PCI-compliant all answers must be Yes, Not Applicable, or (with Security Advisor approval) Compensating Control.



Part 3 and Part 4

Part 3. PCI DSS Validation

Check the status box to indicate the compliance or noncompliance of this Merchant ID.

Check Compliant, if…

- All sections of the SAQ / AOC are complete and;
- All questions answered affirmatively (“YES” or “N/A”), resulting in an overall COMPLIANT rating

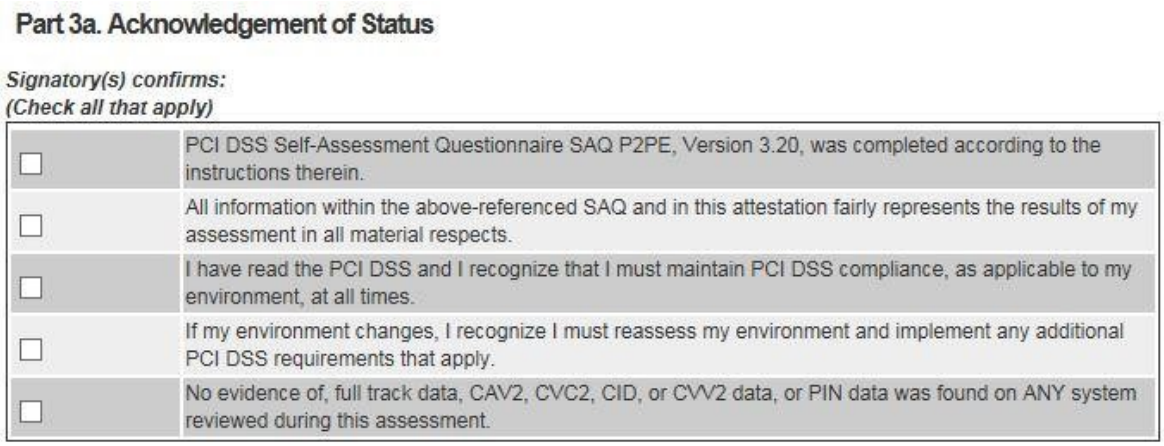
Check Non-Compliant, if…

- Not all sections of the SAQ / AOC are complete or;
- Not all questions are answered "YES” or “N/A

NOTE: If checking Non-Compliant, the merchant manager will be required to complete the Action Plan in Part 4 of this document and enter a Target Date for Compliance. If this is the case, the merchant manager should consult with your University PCI Administrator/Liaison for additional guidance.

Part 3a. Acknowledgement of Status

The merchant manager should be able to confirm the listed statements and check all boxes that apply. To be compliant, you must select all boxes.



Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☐	PCI DSS Self-Assessment Questionnaire SAQ P2PE, Version 3.20, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☐	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
☐	No evidence of, full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data was found on ANY system reviewed during this assessment.

Part 3b. Merchant Attestation

Have the responsible Executive Officer complete and sign this section. Note: this section is verifying the compliance status that is being asserted and that the Executive Officer personally guarantees the validity of the SAQ. Be VERY sure that you have accurately answered all requirements of all sections of the SAQ upon signing this section.

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer (above)		Date:	
Merchant Executive Officer Name:		Title:	

Part 3c. QSA Acknowledgement (if applicable)

It is not necessary to complete Part 3c but if you would like to include CampusGuard's advisory role in the completed SAQ, please work with your CampusGuard CRM to have this section filled in.

Part 3d. ISA Involvement (if applicable)

If your organization has an Internal Security Advisor (ISA) on-staff and they assisted with the completion of the SAQ, you can include their contact details in this section.

Part 4. Action Plan for Non-Compliant Status

Select Yes or No in response to CURRENT STATUS with each section; you should not answer questions based on what you are going to do. The questions should be answered as if the requirement is in-place (Yes) or not in place (No). If No is selected you must add a date of projected compliance. You must also add comments explaining the plan for remediation and compliance.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

Req. 3 - Protect stored cardholder data	○ Yes ◉ No ○ Don't Know Entry of Remediation Date and Action Required.
Req. 9 - Restrict physical access to cardholder data	○ Yes ○ No ○ Don't Know
Req. 12 - Maintain a policy that addresses information security for all personnel	○ Yes ○ No ○ Don't Know

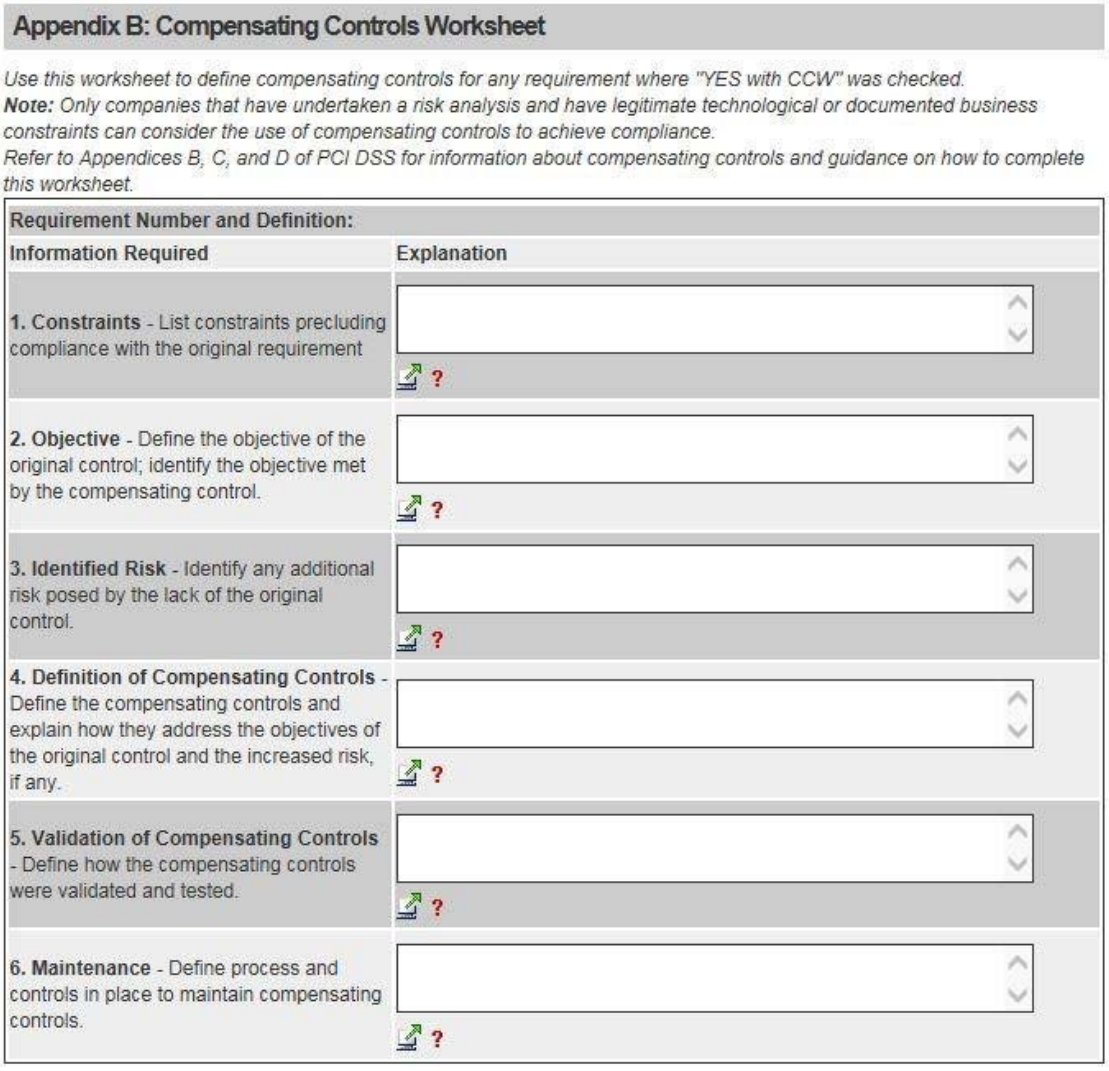
Be sure to click the Save button at the end of each section.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where you chose "Compensating Controls" as the response.

Compensating Controls MUST be approved by your acquiring bank which will require complete documentation of the Compensating Control. Only organizations that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance. A Compensating Control cannot be satisfied by a policy and procedure that already addresses another, existing PCI requirement, and it must go above and beyond the requirement it is trying to satisfy. Compensating Controls need to be re-evaluated on an annual basis.

There are very strict requirements for allowing Compensating Controls, therefore all details need to be annotated and submitted to a QSA for approval. Your CampusGuard Security Advisor and CRM will assist you with the completion of this process.



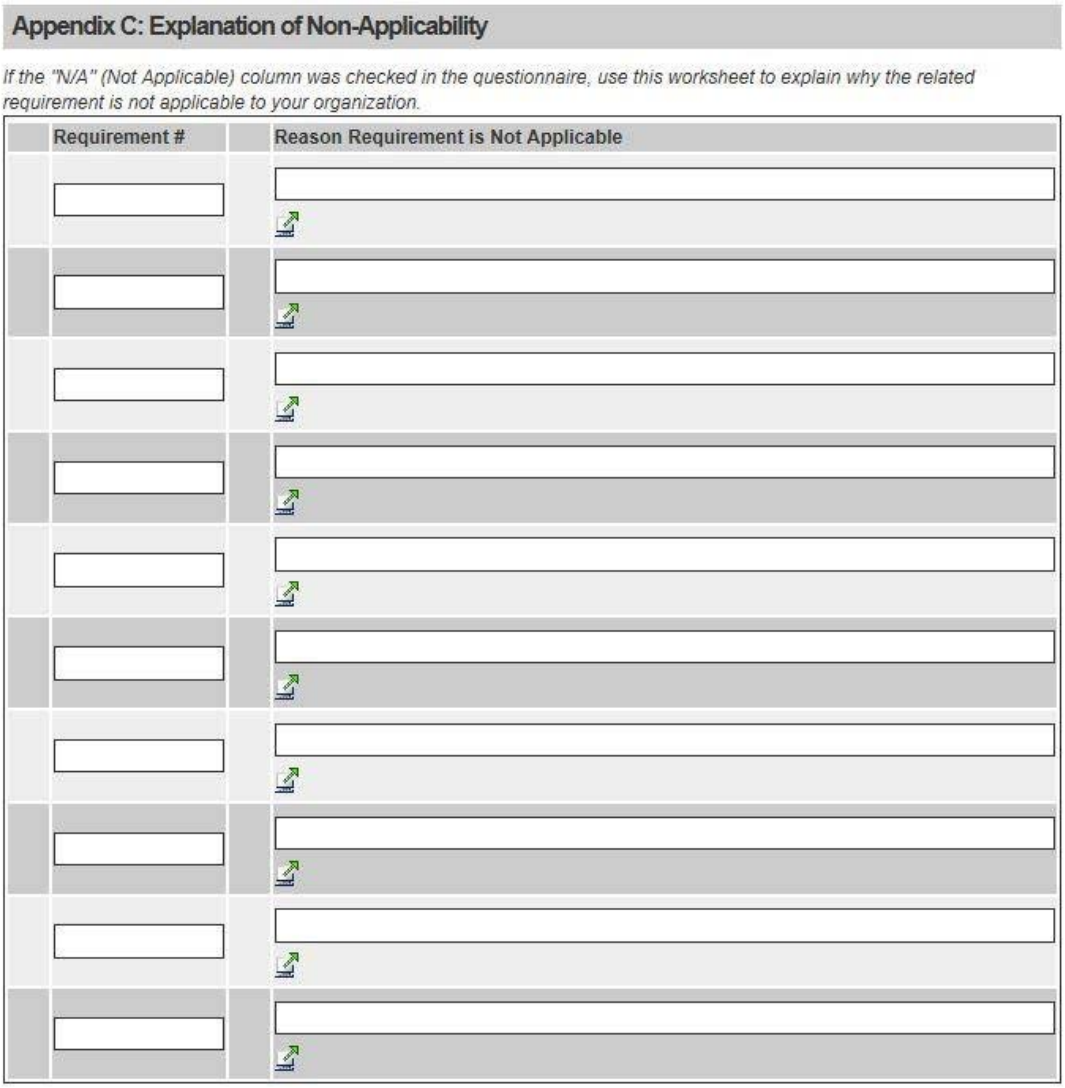
Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.
Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*
Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:	
Information Required	**Explanation**
1. Constraints - List constraints precluding compliance with the original requirement	
2. Objective - Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk - Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls - Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls - Define how the compensating controls were validated and tested.	
6. Maintenance - Define process and controls in place to maintain compensating controls.	

Appendix C: Explanation of Non-Applicability

This appendix is used to explain why a question was answered N/A. You will need to account for every N/A selected throughout the SAQ. In lieu of filling in the page below, you can use a separate document, uploaded to the Document Locker, which follows the format of the screen below.



Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement #	Reason Requirement is Not Applicable