How to Complete Your Self-Assessment Questionnaire (SAQ) and Compliance Documents

The intent of this guidance document is to assist Payment Card Managers in completing their PCI DSS Self-Assessment Questionnaire (SAQ) and Compliance Documents. It should be noted that Payment Card Managers are fully responsible for understanding each question in the SAQ and knowing that their response is accurate within the context of their account(s). The guidance provided in this document is for informational purposes only.

Self-Assessment Questionnaire (SAQ)

The PCI DSS Self-Assessment Questionnaire (SAQ) is an important component of the University's PCI DSS compliance program. The SAQ is an electronic questionnaire consisting of specific technological and procedural questions relating to the security of cardholder data in your area. It provides you with an opportunity to review your operation, think about any changes that have occurred in the last year, and reflect on how your department satisfies PCI DSS requirements.

To maintain compliance with University Policy and PCI DSS, a Self-Assessment Questionnaire (SAQ) has to be completed upon merchant account activation, and then reviewed and updated at the beginning of every fiscal year, or upon any changes to your cardholder data environment.

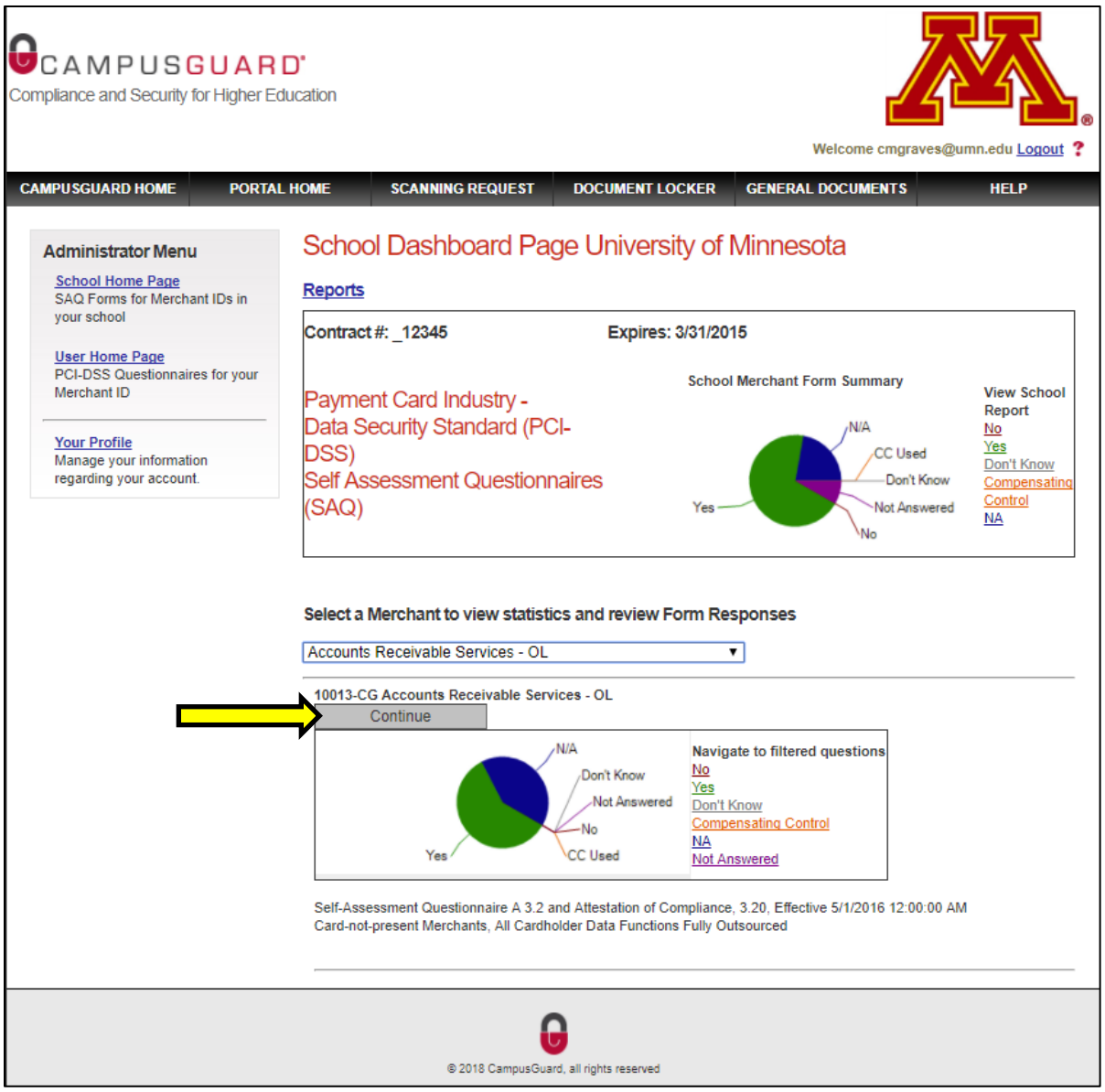
All merchants must comply with the twelve requirements of the Payment Card Industry Data Security Standards (PCI DSS). However, the SAQ for your merchant account(s) may only focus on a specific subset of the requirements, as all the requirements may not be applicable to your payment processes.

How to Complete Your SAQ

The University has an annual support agreement in place with a security assessment firm called CampusGuard to provide resources and expertise needed to achieve and maintain PCI DSS compliance. Included within this agreement is access to a website called the CampusGuard Portal. The CampusGuard Portal is a secure internet-based portal that contains an electronic version of the appropriate PCI DSS Self-Assessment Questionnaire (SAQ) applicable to your merchant account(s).

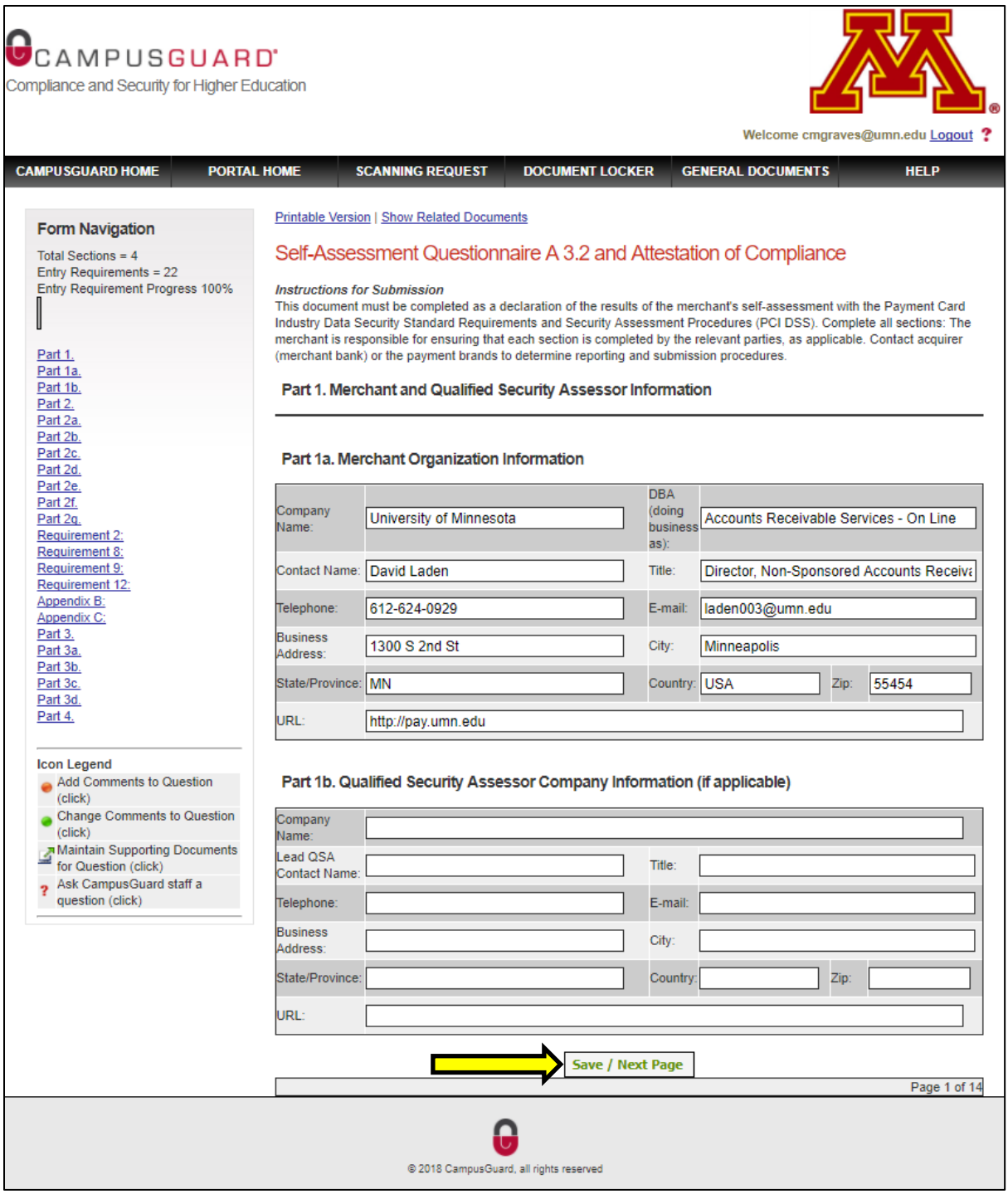
When you were assigned as the Payment Card Manager, you should have received an e-mail from CampusGuard providing you with information and login access to the CampusGuard Portal website. With this login information, you will be able to sign into the CampusGuard Portal website and complete your area's assigned electronic SAQ. You can access your CampusGuard Portal by logging in at https://www.campusguard.com/loginsso.

Once you log into the CampusGuard Portal website, you will see the following page:



To start the review and completion of your assigned SAQ, click on the "**Continue**" button. *Note: If the SAQ has not been completed in the past, this button will be labeled "**Add**", and you would click on the "**Add**" button.*

Once you click on the "**Continue**" button, you will be provided the first page of the SAQ:



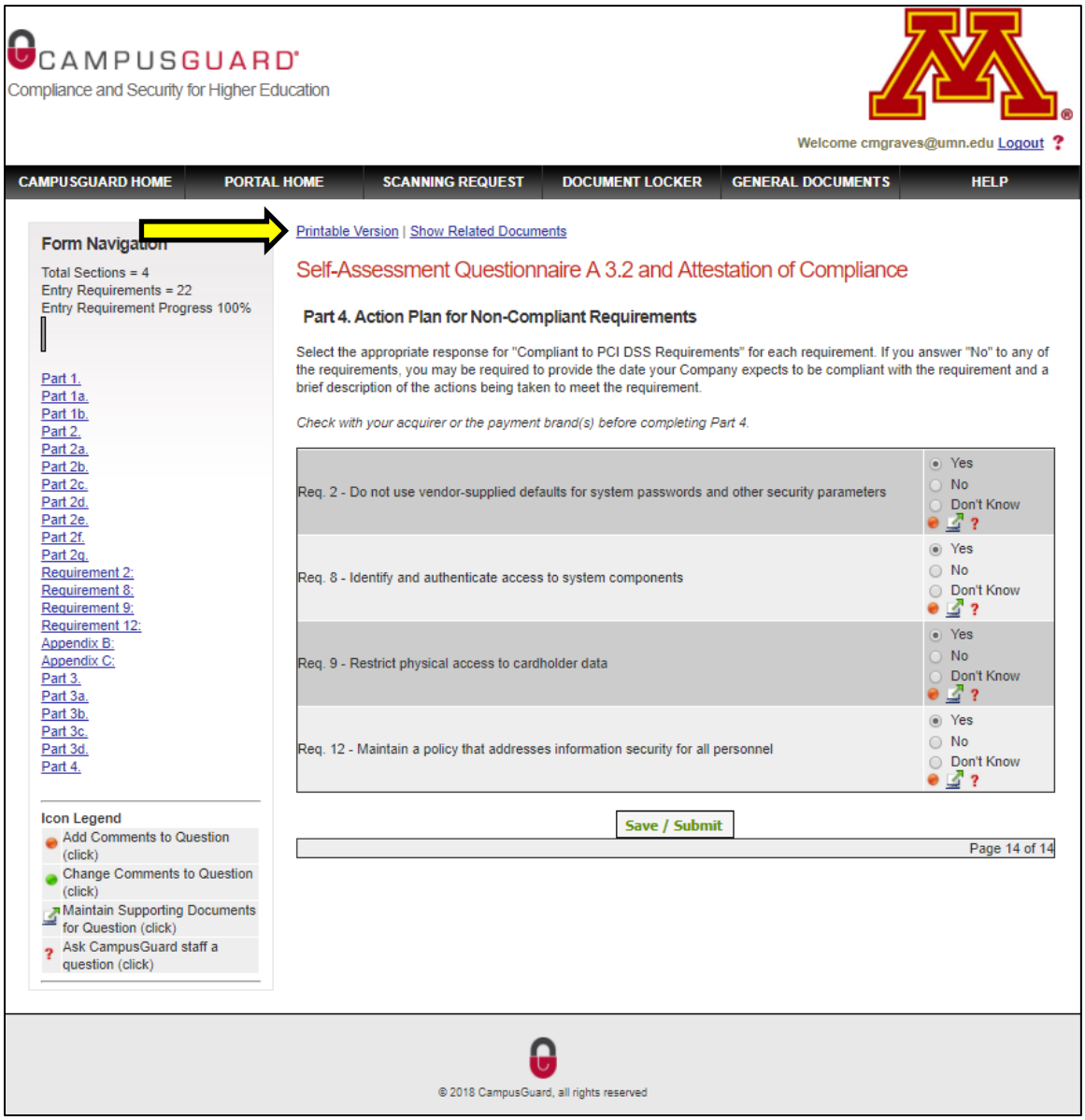
You will now be able to review and update the information shown in your SAQ. *Note: If the SAQ has not been completed in the past, you will need to complete the SAQ as there will be no information pre-populated in the document.*

The SAQ is divided into three distinct sections. The first section is comprised of Parts 1 and 2 of the SAQ, and includes questions about your merchant account and your payment process. The second section of the SAQ contains the PCI DSS requirements. The final section is Part 3 and 4 of the SAQ and is where you certify your compliance with PCI DSS.

Once you have completed each page of your questionnaire, make sure you click on the "**Save / Next Page**" button on the bottom of the page. When you click this button, your information will be saved and you will be taken to the next page of the document.

To assist you in understanding the SAQ questions and accurately answering these questions, the University has a guidance document as well as the user guide provided by CampusGuard, which you may find useful as you are completing your questionnaire. Contact Accounts Receivable Services at pmtcard@umn.edu to receive copies a copy of this guidance.

Once you have completed your SAQ, save a PDF copy of your document. To do this, click on the "**Printable Version**" link at the top of any page, then click the "**Print**" button and print the document as a PDF. Once you have printed as a PDF, you can then upload a copy of the document to your CampusGuard Document Locker.



Compliance Documents

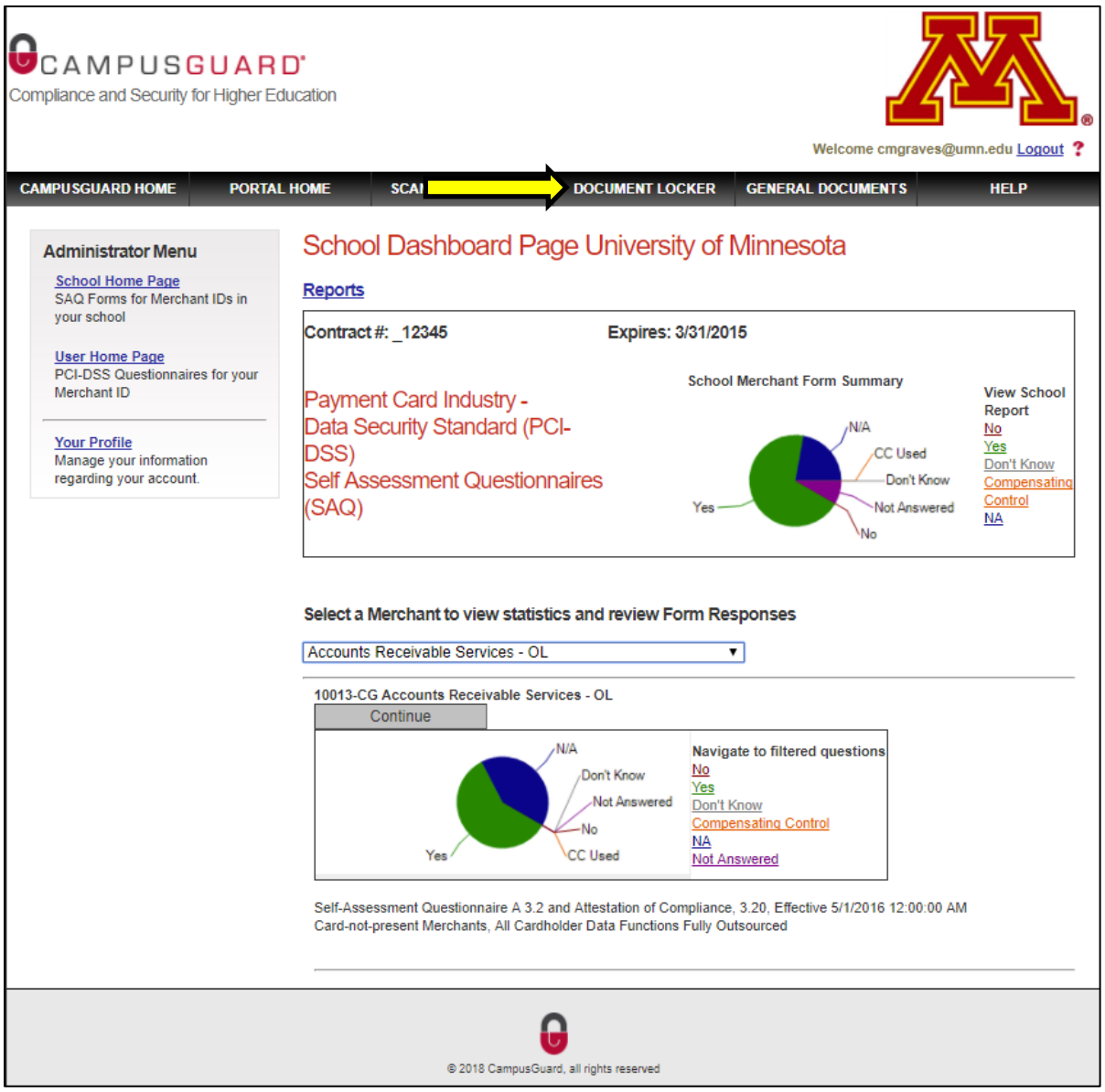
To maintain compliance with University Policy and meet PCI DSS requirements, certain payment card compliance documents are to be completed upon merchant account activation, and then reviewed and updated at the beginning of every fiscal year, or upon any changes to your cardholder data environment. These documents are important as they detail your area's compliance procedures, incident response plan, inventory, data flow, and certify your compliance with PCI DSS.

How to Complete Your Compliance Documents

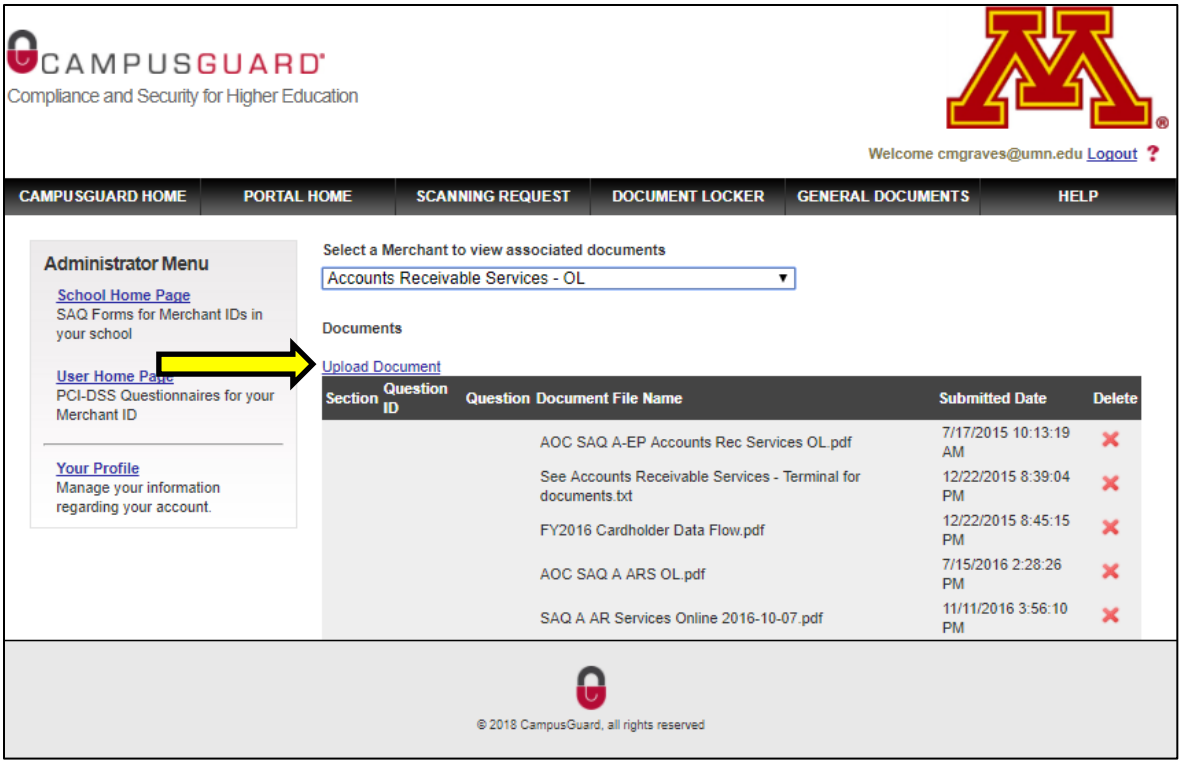
As with your SAQ, the University has an annual support agreement in place with a security assessment firm called CampusGuard to provide resources and expertise needed to achieve and maintain PCI DSS compliance. Included within this agreement is access to a website called the CampusGuard Portal. The CampusGuard Portal is a secure internet-based portal that not only contains an electronic version of the appropriate SAQ applicable to your merchant account(s), but it also includes a section of the portal called the "Document Locker".

When you were assigned as the Payment Card Manager, you should have received an e-mail from CampusGuard providing you with information and login access to the CampusGuard Portal website. With this login information, you will be able to sign into the CampusGuard Portal website and upload your compliance documents to the "Document Locker". You can access your CampusGuard Portal by logging in at https://www.campusguard.com/loginsso.

To access your Document Locker, log into the CampusGuard Portal website, then click on the "**Document Locker**" link in the black bar at the top of the page.



Once you click on the "Document Locker" link, you will be taken to the locker for your merchant account. The Document Locker is a cloud drive where you store all your payment card compliance documents.



To upload a document to the Document Locker, all you need to do is click on the "**Upload Document**" link at the top left of the page. It is recommended that you upload copies of your compliance documentation in the format they were created. You do not need to transfer your documents to a PDF prior to upload.

The following are the seven compliance documents which need to completed at the time of assignment and annually thereafter:

1. Department Payment Card Manager Form (UM 1624)
   The Department Payment Card Manager Form certifies that the Payment Card Manager is knowledgeable about the payment card acceptance process in the unit, responsible for required compliance documentation and ensuring that all PCI DSS requirements are met, and is the first point of contact for all questions concerning the payment card account(s). This form can be found in the University Forms Library at http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1624.doc, and should be completed, signed, and uploaded to the CampusGuard Document Locker upon your assignment as Payment Card Manager. The Department Payment Card Manager form automatically expires at the end of the fiscal year and must be renewed annually.

2. Employee Non-Disclosure Form (UM 1623)
   The Employee Non-Disclosure Form certifies that the signer of the form has been identified as an employee involved in the payment transaction process who may have access to confidential information related to payment cards. The signer agrees to only use the cardholder information for the intended business purpose of the department; to use their best efforts to prevent and protect any part of the cardholder information from disclosure to the public domain or into the possession of unauthorized persons; that they have read and will abide by associated University policies, laws, and standards; and that they have been trained on the importance of protecting cardholder data. This form can

be found in the University Forms Library at http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1623.doc, and should be completed and signed by all employees involved in the payment card process. These forms should then be uploaded to the CampusGuard Document Locker. The Employee Non-Disclosure Form automatically expires at the end of the fiscal year and must be renewed annually.

3. Incident Response and Continuity Plan (UM 1634)

The Incident Response and Continuity Plan details your department's security incident response plan that must be invoked when a security incident involving payment cards has been identified. This form can be found in the University Forms Library at http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1634.doc, and should be completed, signed, and uploaded to the CampusGuard Document Locker upon your assignment as Payment Card Manager. The Incident Response and Continuity Plan automatically expires at the end of the fiscal year and must be renewed annually.

Note: If this is not a new merchant account, and you are replacing the previous Payment Card Manager, you may be able to update your area's current Incident Response and Continuity Plan, in lieu of creating a new document. A copy of the current Incident Response and Continuity Plan should be found in your CampusGuard Document Locker.

4. Payment Card Operational Procedures

The Payment Card Operational Procedures document explains the specific payment card transaction processes for your area, required training of employees processing payment cards in your area, security of payment card devices in your area, as well as other information pertinent to your area's payment card processing. A template operating procedures document can be found on the University's Payment Card Industry Data Security Standards (PCI DSS) website at http://controller.umn.edu/business-processes/AR10.html. This document should be completed upon your assignment as Payment Card Manager, making sure the template information is updated to reflect your area's specific payment card processes. Once completed, this document should be uploaded to the CampusGuard Document Locker. The Payment Card Operational Procedures document must be reviewed, updated (if needed), re-dated, and uploaded to the CampusGuard Document Locker at the beginning of each fiscal year.

Note: If this is not a new merchant account, and you are replacing the previous Payment Card Manager, you may be able to review, update (if needed), and re-date your area's current Payment Card Operational Procedures document, in lieu of creating a new document. A copy of the current Payment Card Operational Procedures document should be found in your CampusGuard Document Locker.

5. Cardholder Data Flow Chart

The Cardholder Data Flow Chart documents how and where payment card information is stored, processed, or transmitted within your environment, as well as identifying all supporting and connected systems and devices. A sample cardholder data flow chart can be found on the University's Payment Card Industry Data Security Standards (PCI DSS) website at http://controller.umn.edu/business-processes/AR10.html. This document should be completed upon your assignment as Payment Card Manager, making sure the flow chart reflects your area's specific payment card processes. Once completed, this document should be uploaded to the CampusGuard Document Locker. The Cardholder Data Flow Chart must be reviewed, updated (if needed), re-dated, and uploaded to the CampusGuard Document Locker at the beginning of each fiscal year.

Note: If this is not a new merchant account, and you are replacing the previous Payment Card Manager, you may be able to review, update (if needed), and re-date your area's current Cardholder Data Flow Chart, in lieu of creating a

new document. A copy of the current Cardholder Data Flow Chart should be found in your CampusGuard Document Locker.

6. Payment Card Inventory List

   The Payment Card Inventory List documents all payment card devices within your environment. This inventory list should, at a minimum, determine the owner, provide contact information, and explain the purpose of the device. If your area utilizes an internet payment gateway such as Authorize.net, your inventory list should include information on the University or Third-Party server hosting the website which redirects the customer to the payment page website. A template payment card inventory list can be found on the University's Payment Card Industry Data Security Standards (PCI DSS) website at http://controller.umn.edu/business-processes/AR10.html. This document should be completed upon your assignment as Payment Card Manager, making sure the template information is updated to reflect your area's specific payment card processes. Once completed, this document should be uploaded to the CampusGuard Document Locker. The Payment Card Inventory List must be reviewed, updated (if needed), re-dated, and uploaded to the CampusGuard Document Locker at the beginning of each fiscal year.

   Note: If this is not a new merchant account, and you are replacing the previous Payment Card Manager, you may be able to review, update (if needed), and re-date your area's current Payment Card Inventory List, in lieu of creating a new document. A copy of the current Payment Card Inventory List should be found in your CampusGuard Document Locker.

7. Payment Card Manager Compliance Certification Form

   The Payment Card Manager Compliance Certification Form certifies that the Payment Card Manager has completed all the required compliance documents and forms, and that these documents have been uploaded to the CampusGuard Document Locker. This form can be found on the University's Payment Card Industry Data Security Standards (PCI DSS) website at http://controller.umn.edu/business-processes/AR10.html, and should be completed, signed, and uploaded to the CampusGuard Document Locker upon your assignment as Payment Card Manager. The Payment Card Manager Compliance Certification Form automatically expires at the end of the fiscal year and must be renewed annually.

If you have any questions, contact Accounts Receivable services at pmtcard@umn.edu.