# Table of Contents

How to Complete Your Self-Assessment Questionnaire (SAQ) and Accompanying Compliance Documents ............ 3  
Self-Assessment Questionnaire (SAQ) A and Attestation of Compliance Guidance ...........................................11  
Self-Assessment Questionnaire (SAQ) B and Attestation of Compliance Guidance ......................................... 26  
Self-Assessment Questionnaire (SAQ) P2PE and Attestation of Compliance Guidance .................................... 41  
SAQ Frequently Asked Questions ......................................................................................................................... 55  
Resources .................................................................................................................................................................. 60
How to Complete Your Self-Assessment Questionnaire (SAQ) and Accompanying Compliance Documents

The intent of this guidance document is to assist University of Minnesota Payment Card Managers in completing their PCI DSS Self-Assessment Questionnaire (SAQ) and accompanying 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).

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.

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, and requires you to answer specific questions related to these data security requirements. The final section is Part 3 and 4 of the SAQ, and is where you certify your area’s compliance with PCI DSS.

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.

The University has a 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).

CampusGuard Portal
To assist departments and the University with our payment card compliance, there is a 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 their CampusGuard Portal, which allows University merchants to complete and save PCI DSS compliance questionnaires and associated compliance
The CampusGuard Portal is a secure website containing an electronic version of the appropriate PCI DSS Self-Assessment Questionnaire (SAQ) for your account(s). Within the CampusGuard Portal is a separate section called the Document Locker, which allows you to electronically store critical documents required for PCI DSS compliance. These documents are retained in the Document Locker for reference and verification by your department, Accounts Receivable Services, and CampusGuard. You can access your area’s CampusGuard Portal at http://portal.campusguard.com/loginso.

How to Complete Your SAQ

You can access electronic versions of the Self-Assessment Questionnaire(s) for your account(s) by logging into the CampusGuard Portal at http://portal.campusguard.com/loginso.

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. If the SAQ has not been completed in the past, it will be blank and you will need to populate all areas of the electronic 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, and requires you to answer specific questions related to these data security requirements. The final section is Part 3 and 4 of the SAQ, and is where you certify your area’s 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.

Resources to assist you with completion of your SAQ(s) 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.

Once you have completed your SAQ, it is important to 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 (for information on how to upload a document to the CampusGuard Document Locker, see the “How to Complete Your Compliance Documents” section below).
Accompanying Compliance Documents

To maintain compliance with University Policy and PCI DSS, it is required that certain payment card compliance documents be completed at least annually and uploaded to the CampusGuard Document Locker. 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.

These compliance documents have to be completed upon merchant account activation, and then reviewed and updated at least annually, or upon any changes to your cardholder data environment, such as the appointment of a new Payment Card Manager.

How to Complete Your Accompanying Compliance Documents

As with your SAQ, the University has a 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”.

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 document locker associated with your merchant account. The Document Locker is a cloud drive where you can store all your payment card compliance documents.

![Image of Document Locker interface](image)

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 accompanying compliance documents which need to completed whenever a new merchant account is assigned, and annually thereafter. After completion of these documents, they should be uploaded to the CampusGuard Document Locker.

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). The Department Payment Card Manager Form can be found in the University Forms Library at [http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1624.doc](http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1624.doc).
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. The Employee Non-Disclosure Form can be found in the University Forms Library at [http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1623.doc](http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1623.doc).

3. **Incident Response and Continuity Plan (UM 1634)**
   The Incident Response and Continuity Plan details your department’s security incident response plan, which must be invoked when a security incident involving payment cards has been identified. The Incident Response and Continuity Plan form can be found in the University Forms Library at [http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1634.doc](http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1634.doc).

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 Payment Card Operational 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](http://controller.umn.edu/business-processes/AR10.html).

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](http://controller.umn.edu/business-processes/AR10.html).

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](http://controller.umn.edu/business-processes/AR10.html).
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. The Payment Card Manager Compliance Certification 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.

If you have any questions regarding these compliance documents, contact Accounts Receivable Services at pmtcard@umn.edu.
Self-Assessment Questionnaire (SAQ) A and Attestation of Compliance Guidance

The intent of this guidance is to assist University of Minnesota Payment Card Managers in completing their PCI DSS Self-Assessment Questionnaire (SAQ). Specifically, this document is for use with accounts that qualify to complete an SAQ A (see description below). 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 A

**SAQ Description:** 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. The SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data. SAQ A merchants are e-commerce merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

- You accept only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- You do not electronically store, process, or transmit any cardholder data on your systems or premises, but rely entirely on a third party(s) to handle all these functions;
- You have confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.

*Additionally, for e-commerce channels:*

- All elements of the payment page(s) delivered to your consumer’s browser originate only and directly from a PCI DSS validated third-party service provider(s).

*This SAQ is not applicable to face-to-face channels.*

**Note:** If your merchant account utilizes Authorize.net as a payment gateway, and your integration method is not a Server Integration Method (SIM) or Accept Hosted Integration, contact the Payment Card Program at pmtcard@umn.edu as you may need to complete a different SAQ (SAQ A-EP or SAQ D).

All merchants must comply with all twelve requirements of the Payment Card Industry Data Security Standards (PCI DSS). However, the self-assessment for SAQ A merchants focuses on the following requirements:
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 6: Develop and maintain secure systems and applications

Requirement 8: Identify and authenticate access to system components

Requirement 9: Restrict physical access to cardholder data

Requirement 12: Maintain a policy that addresses information security for all personnel

Note: For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, and 8) apply to e-commerce merchants that redirect customers from their website to a third party for payment processing, and specifically to the merchant web server upon which the redirection mechanism is located. Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the third party) and therefore do not have any systems in scope for this SAQ, would consider these requirements to be “not applicable.”

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) for your account(s). This electronic SAQ allows you to complete your questionnaire online. You can access your CampusGuard Portal by logging in at http://portal.campusguard.com/loginsso.

For each question, there is a choice of responses to indicate your area’s status regarding that requirement. Only one response should be selected for each question. A description of the meaning for each response is provided in the table below.

<table>
<thead>
<tr>
<th>Response</th>
<th>When to use this response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>The expected testing has been performed, and all elements of the requirement have been met as stated.</td>
</tr>
<tr>
<td>No</td>
<td>Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>Selecting this response would mean your area is not compliant with PCI DSS requirements.</td>
</tr>
<tr>
<td></td>
<td>If you do not know the answer to the requirement, contact <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> for guidance prior to selecting this response.</td>
</tr>
<tr>
<td></td>
<td>Selecting this response would mean your area is not compliant with PCI DSS requirements.</td>
</tr>
</tbody>
</table>
Not Applicable (N/A)  The requirement does not apply to the environment.

All responses in this column require a supporting explanation in Appendix C of the SAQ.

Compensating Control Used  The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.

As all responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ, contact pmtpcard@umn.edu for guidance prior to selecting this response.

Guidance for Completing Your SAQ: The following chart offers guidance and helpful hints, which may be useful as you are completing your Self-Assessment Questionnaire.

<table>
<thead>
<tr>
<th>Section 1: Assessment Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAQ Section or Question</strong></td>
</tr>
<tr>
<td><strong>Merchant and Qualified Security Assessor Information</strong></td>
</tr>
<tr>
<td>Part 1a. Merchant Organization Information</td>
</tr>
<tr>
<td>Part 1b. Qualified Security Assessor Company Information (if applicable)</td>
</tr>
<tr>
<td><strong>Executive Summary</strong></td>
</tr>
<tr>
<td>Part 2a. Type of Merchant Business (check all that apply)</td>
</tr>
</tbody>
</table>
| Part 2b. Description of Payment Card Business | Describe your payment card environment in detail. Be sure to include an explanation of:  
  • What the customer is purchasing,
- How you process credit card payments (your payment card environment), and
- Any service provider(s) and how they interact with your payment card environment.
- If you store payment card information electronically or on paper, explain how and why this is done.

An example description may be, “The department has a merchant account which allows us to accept credit and debit card payments for our online supplemental application fee. The customer is directed to the department’s online application website, where they complete their application and are automatically redirected to our payment gateway (Authorize.net) for processing of their payment card.

### Part 2c. Locations

Describe the type of facility included in your PCI DSS review.

Most often, the type of facility for SAQ A merchants is limited to “Office or Departmental Setting” as your process involves online sales.

### Part 2d. Payment Application

Payment Applications are systems or software that are:
- Hosted and managed by the University, and
- Used to store, process, or transmit cardholder data electronically.

An example of a Payment Application is a Point of Sale system.

*Most often, for SAQ A merchants, there are no payment applications being used as you are processing payments through the use of a third-party payment gateway, such as Authorize.net.*

### Part 2e. Description of Environment

“Provide a high-level description of the environment covered by this assessment.”

Most often, a high-level description of an SAQ A environment is limited to a statement such as “For payment card transactions, the department uses a University website redirecting to Authorize.net (a PCI DSS validated third-party payment processor)”.

“Does your business use network segmentation to affect the scope of your PCI DSS environment?”
| Part 2f. Third-Party Service Providers | “Does your company use a Qualified Integrator & Reseller (QIR)?”

For SAQ A merchants, you most likely do not use a Qualified Integrator and Reseller Company (QIR Company) to implement, configure, and/or support your payment card applications, so the answer to this question would be “No.”

“Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?”

A third-party service provider is any company that stores, transmits, or processes payment cards for the University; or any entity that can affect the security of cardholder data.

Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, PayPal, RegOnline, and others.

Make sure to list all third-party service providers that your area uses to store, transmit, or process payment cards.

Note: Requirement 12.8 applies to all entities in this list. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 2g. Eligibility to Complete AOC SAQ A</td>
<td>Carefully read each of the six statements. Check each statement that is true for your account. If any statements are not true for your account, or if you are unsure, contact Accounts Receivable Services at <a href="mailto:pmntcard@umn.edu">pmntcard@umn.edu</a>.</td>
</tr>
</tbody>
</table>

---

**Section 2: Self-Assessment Questionnaire**

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.
2.1 (a) Are vendor-supplied defaults always changed before installing a system on the network?
This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer “Yes” to this question if both of the following are correct:

1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure for vendor-supplied defaults to always be changed.

2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure for vendor-supplied defaults to always be changed.

2.1 (b) Are unnecessary default accounts removed or disabled before installing a system on the network?

As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer “Yes” to this question if the following is correct:

1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that unnecessary default accounts are removed or disabled before installing a system on the network.

2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that unnecessary default accounts are removed or disabled.

**Requirement 6: Develop and maintain secure systems and applications**

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and
compromise of cardholder data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

| 6.2 (a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches? | There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data. Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. This requirement applies to applicable patches for system components and software in the cardholder environment, including websites, hosting providers, and payment processing. As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to these questions if the following is correct:

1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, applicable vendor-supplied security patches are installed, and critical security patches are installed within one month of release.
2. You can confirm that, for the payment gateway which processes your online credit card payments, applicable vendor-supplied security patches are installed, and critical security patches are installed within one month of release. |
| 6.2 (b) Are critical security patches installed within one month of release? | |
**Requirement 8: Identify and authenticate access to system components**

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

| 8.1.1 Are all users assigned a unique ID before allowing them to access system components or cardholder data? | As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer “Yes” to this question if the following is correct:
3. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that all users are assigned a unique ID before allowing them to access the server.
4. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that all users are assigned a unique ID before allowing them to access the payment gateway. |
| 8.1.3 Is access for any terminated users immediately deactivated or removed? | As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer “Yes” to this question if the following is correct:
1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that access to the server for any terminated users is immediately deactivated or removed.
2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that access to the gateway for any terminated users is immediately deactivated or removed. |
| 8.2 In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? | As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer “Yes” to this question if the following is correct:
- **Something you know, such as a password or passphrase** |
• Something you have, such as a token device or smart card
• Something you are, such as a biometric

1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure to authenticate users with a unique ID, as well as something you know, something you have, or something you are.
2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure to authenticate users with a unique ID, as well as something you know, something you have, or something you are.

8.2.3 (a) Are user password parameters configured to require passwords/passphrases meet the following?
• A minimum password length of at least seven characters
• Contain both numeric and alphabetic characters
Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.5 Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows?
• Generic user IDs and accounts are disabled or removed;
• Shared user IDs for system administration activities and other critical functions do not exist; and
• Shared and generic user IDs are not used to administer any system components?

As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer “Yes” to this question if the following is correct:
1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that user’s password parameters include a minimum length of seven characters and contain both numeric and alphabetic characters.
2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that user’s password parameters include a minimum length of seven characters and contain both numeric and alphabetic characters.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically
present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

Two common findings are (1) the need to recognize where increased security is required, and (2) to document all operational procedures in writing.

### 9.5 Are all media physically secured?
*(media includes computers, removable electronic media, hard drives, portable drives, USB sticks, CDs, DVDs, paper reports, paper receipts, and faxes)*

Because SAQ-A merchants do not typically interact with any media containing cardholder data, this item is typically marked “Not Applicable (N/A)”. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer’s data at their request. In short, SAQ-A merchants should never see or have access to full card numbers.

If this is not the case with your account, you may need to answer this question “NO” and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.

### 9.6 (a) Is strict control maintained over the internal or external distribution of any kind of media?

### 9.6 (b) Do controls include the following:
- 9.6.1 Is media classified so the sensitivity of the data can be determined?
- 9.6.2 Is media sent by secured courier or other delivery method that can be accurately tracked?
- 9.6.3 Is management approval obtained prior to moving the media?

Typically, this is answered as “Not Applicable (N/A)” as SAQ-A merchants do not typically interact with any media containing cardholder data. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer’s data at their request. In short, SAQ-A merchants should never see or have access to full card numbers.

If this is not the case with your account, you may need to answer this question “NO” and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.

### 9.7 Is strict control maintained over the storage and accessibility of media?

Typically, this is answered as “Not Applicable (N/A)” as SAQ-A merchants do not typically interact with any media containing cardholder data. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer’s data at their request. In short, SAQ-A merchants should never see or have access to full card numbers.

If this is not the case with your account, you may need to answer this question “NO” and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.
<table>
<thead>
<tr>
<th>Requirement 12: Maintain a policy that addresses information security for all personnel</th>
</tr>
</thead>
</table>
| 9.8 (a) Is all media destroyed when it is no longer needed for business or legal reasons?  
9.8 (c) Is media destruction performed as follows:  
9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?  
9.8.1 (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents? |
| Typically, this is answered as “Not Applicable (N/A)” as SAQ-A merchants do not typically interact with any media containing cardholder data. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer’s data at their request. In short, SAQ-A merchants should never see or have access to full card numbers.  
If this is not the case with your account, you may need to answer this question “NO” and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan. |

**A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.**

A common concern in this area is ensuring that merchants maintain adequate payment card procedures which include explanations on employee training and termination, how customers pay for purchases, disposal of cardholder data, and incident response.

*Note: Each merchant must have a written statement in their operational procedures stating they comply with University of Minnesota Information Security Policies and Procedures.*

<table>
<thead>
<tr>
<th>12.8.1 Is a list of service providers maintained?</th>
</tr>
</thead>
</table>
| As SAQ-A accounts are e-commerce accounts, your process normally involves a third party service provider supplying the payment gateway which processes your online credit card payments. Your process may also involve a third party service provider which hosts the website that redirects to your payment gateway for processing.  
*Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, and others.* |

*Note: A third-party service provider is any company that stores, transmits, or processes payment cards for the University, as well as any company that could affect the security of a cardholder transaction.*
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.8.2 Is a written agreement maintained that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess?</td>
<td>For University-wide third party service providers such as Authorize.net and AudienceView, this agreement is created and maintained through the vendor contract which typically involves Purchasing, OGC, and the Controller’s Office. If your account uses a third party service provider, you should have worked with Accounts Receivable Services (ARS) to ensure that an appropriate agreement was established and that a copy of the most recent agreement was provided to ARS. The answer to this question should be “Yes”, as the Accounts Receivable Services department maintains a written agreement with the service provider. For PCI DSS compliance purposes, the Payment Card Manager must know that this agreement exists and that it can be found in the Accounts Receivable Services department.</td>
</tr>
<tr>
<td>12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?</td>
<td>The University’s Accounts Receivable Services Department, Purchasing Department, and Office of General Counsel (OGC) all have an established process for engaging service providers that interact with cardholder data on behalf of the University. The Payment Card Manager must be aware that all of these areas have an established process in place for engaging payment card service providers prior to the use of the service provider…and this established process must be utilized whenever new payment card service providers are to be introduced to your environment. The answer to this question should be “Yes”, as the Accounts Receivable Services department maintains an established process for engaging service providers.</td>
</tr>
<tr>
<td>12.8.4 Is a program maintained to monitor service providers’ PCI DSS compliance status?</td>
<td>The answer to this question should be “Yes”, as the Accounts Receivable Services department monitors the service providers’ PCI DSS compliance via contractual language.</td>
</tr>
<tr>
<td>12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider?</td>
<td>The answer to this question should be “Yes”, as the Accounts Receivable Services department works with the service provider to ensure that appropriate requirements are managed by all parties.</td>
</tr>
<tr>
<td>12.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?</td>
<td>If you maintain and annually review the UM1634 Form “Incident Response and Continuity Plan”, you can typically answer “Yes” to this question. Keep in mind that this form has to be uploaded to the CampusGuard Document Locker annually as well.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Appendix B: Compensating Controls Worksheet</strong></td>
<td>Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: 1) Meet the intent and rigor of the original stated PCI DSS requirement; 2) Provide a similar level of defense as the original PCI DSS requirement; 3) Be &quot;above and beyond&quot; other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. If you answered “Compensating Control Used” to any of the questions shown in the requirement sections, contact <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> for further guidance on how to complete this section. Typically, merchants do not use compensating controls, so this section can be left blank.</td>
</tr>
<tr>
<td><strong>Appendix C: Explanation of Non-Applicability</strong></td>
<td>If you answered “Not Applicable (N/A)” to any of the questions shown in the requirement sections, you are required to use this worksheet to explain why the related requirement is not applicable to your area.</td>
</tr>
<tr>
<td><strong>Section 3: Validation and Attestation Details</strong></td>
<td>After completing the body of the SAQ, if you answered “Yes” or “Not Applicable (N/A)” to all the questions asked in the requirements sections, your area is compliant and you can check the “Compliant” box.</td>
</tr>
<tr>
<td><strong>Part 3a. Acknowledgement of Status</strong></td>
<td>After completing the body of the SAQ carefully read each of the statements shown in this section, and check each statement that is true for your account.</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• <strong>PCI DSS Self-Assessment Questionnaire A, Version 3.20,</strong> was completed according to the instructions therein.</td>
</tr>
<tr>
<td></td>
<td>• All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.</td>
</tr>
</tbody>
</table>
| | • I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.  
  *For this SAQ, all payment processing functions are fully outsourced to a third party such as Authorize.net. If you utilize Authorize.net as your payment processor, you can typically check this box as Authorize.net does not store sensitive authentication data after authorization. If your area uses a payment processor other than Authorize.net, you will need to check with that processor to verify that they do not store sensitive authentication data after authorization.* |
| | • 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 storage after transaction authorization was found on ANY system reviewed during this assessment.  
  *If your payment process utilizes the use of Authorize.net, you can typically check this box as Authorize.net does not store full track data, CAV2,
CVC2, CID, CVV2 data, or PIN data after authorization.

- ASV scans are being completed by the PCI SSC Approved Scanning Vendor

  As ASV scans are not required for merchants redirecting to a payment processor for payment, you should be able to leave this question blank.

If you are unsure about any of the questions shown in this section, contact the Payment Card Program at pmtcard@umn.edu.

<table>
<thead>
<tr>
<th>Part 3b. Merchant Attestation</th>
<th>After completing the body of the SAQ the Payment Card Manager is to type in the current date, and enter their name and title as the “Merchant Executive Officer”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 3c. QSA Acknowledgement (if applicable)</td>
<td>This section does not need to be completed.</td>
</tr>
<tr>
<td>Part 3d. ISA Acknowledgement (if applicable)</td>
<td>This section does not need to be completed.</td>
</tr>
<tr>
<td>Part 4. Action Plan for Non-Compliant Status</td>
<td>This section is a summary of the PCI DSS requirements shown in your questionnaire. If you answered “Yes” or “Not Applicable (N/A)” to all the questions asked in the requirements sections, your area is compliant and you can check “Yes” for each line item.</td>
</tr>
</tbody>
</table>

If you answered “No” to any of the questions asked in the requirements sections, your area is non-compliant and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section.
Self-Assessment Questionnaire (SAQ) B and Attestation of Compliance Guidance

The intent of this guidance is to assist University of Minnesota Payment Card Managers in completing their annual PCI DSS Self-Assessment Questionnaire (SAQ) and Attestation of Compliance. Specifically, this document is for use with accounts that qualify to complete an SAQ B (see description below). 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 B

SAQ Description: 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. The SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B merchants confirm that, for this payment channel:
- You use only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers’ payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- You do not transmit cardholder data over a network (either an internal network or the Internet);
- You retain only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and
- You do not store cardholder data in electronic format.

All merchants must comply with all twelve requirements of the Payment Card Industry Data Security Standards (PCI DSS). However, the self-assessment for SAQ B merchants focuses on portions of five standards:

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 7: Restrict access to cardholder data by business need to know

Requirement 9: Restrict physical access to cardholder data

Requirement 12: Maintain a policy that addresses information security for all personnel
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) for your account(s). This electronic SAQ allows you to complete your questionnaire online. You can access your CampusGuard Portal by logging in at http://portal.campusguard.com/loginssso.

For each question, there is a choice of responses to indicate your area’s status regarding that requirement. Only one response should be selected for each question. A description of the meaning for each response is provided in the table below.

<table>
<thead>
<tr>
<th>Response</th>
<th>When to use this response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>The expected testing has been performed, and all elements of the requirement have been met as stated.</td>
</tr>
<tr>
<td>No</td>
<td>Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.</td>
</tr>
<tr>
<td></td>
<td><strong>Selecting this response would mean your area is not compliant with PCI DSS requirements.</strong></td>
</tr>
<tr>
<td>Don’t Know</td>
<td>If you do not know the answer to the requirement, contact <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> for guidance prior to selecting this response.</td>
</tr>
<tr>
<td></td>
<td><strong>Selecting this response would mean your area is not compliant with PCI DSS requirements.</strong></td>
</tr>
<tr>
<td>Not Applicable (N/A)</td>
<td>The requirement does not apply to the environment.</td>
</tr>
<tr>
<td></td>
<td><strong>All responses in this column require a supporting explanation in Appendix C of the SAQ.</strong></td>
</tr>
<tr>
<td>Compensating Control Used</td>
<td>The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.</td>
</tr>
<tr>
<td></td>
<td>As all responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ, contact <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> for guidance prior to selecting this response.</td>
</tr>
</tbody>
</table>

Guidance for Completing Your SAQ: The following chart offers guidance and helpful hints, which may be useful as you are completing your Self-Assessment Questionnaire.
## Section 1: Assessment Information

<table>
<thead>
<tr>
<th>SAQ Section or Question</th>
<th>Helpful Hints &amp; Common Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Merchant and Qualified Security Assessor Information</strong></td>
<td>Complete this section with the contact information for your merchant area/department including the contact information for the merchant manager who has responsibility for the merchant account and the payment card activities in the office.</td>
</tr>
<tr>
<td>Part 1a. Merchant Organization Information</td>
<td><strong>Note:</strong> Company Name should be “Regents of the University of Minnesota”, and DBA (doing business as) should be your Payment Card Account Name.</td>
</tr>
<tr>
<td>Part 1b. Qualified Security Assessor Company Information (if applicable)</td>
<td>Since the University rolls our SAQs up into a single report to submit to our acquiring bank you can leave this section blank.</td>
</tr>
<tr>
<td><strong>Executive Summary</strong></td>
<td>Select the type of business that is applicable to your area or department.</td>
</tr>
<tr>
<td>Part 2a. Type of Merchant Business (check all that apply)</td>
<td>Check the types of credit and debit card payment channels that your area uses.</td>
</tr>
<tr>
<td></td>
<td>Check the types of payment channels that are covered by this SAQ. Most often, this is limited to “MOTO” and/or “Card-present (face-to-face)” for SAQ-B merchants. If you are completing this SAQ for an e-commerce account as well as a dial-up or cellular terminal, you may want to select “E-Commerce” as well as “MOTO” and/or “Card-present (face-to-face).”</td>
</tr>
<tr>
<td>Part 2b. Description of Payment Card Business</td>
<td>Describe your payment card environment in detail. Be sure to include an explanation of:</td>
</tr>
<tr>
<td></td>
<td>- <em>What the customer is purchasing,</em></td>
</tr>
<tr>
<td></td>
<td>- <em>How you process credit card payments (your payment card environment), and</em></td>
</tr>
<tr>
<td></td>
<td>- <em>Any service provider(s) and how they interact with your payment card environment.</em></td>
</tr>
<tr>
<td></td>
<td>- <em>If you store payment card information electronically or on paper, explain how and why this is done.</em></td>
</tr>
<tr>
<td></td>
<td>An example description may be, “The department has a merchant account for two dial-up swipe terminals which allows us to accept credit and debit card payments for the sales of admission fees as well as merchandise. The customer can pay in-person or via phone call.”</td>
</tr>
</tbody>
</table>
| Part 2c. Locations | Describe the type of facility included in your PCI DSS review.  
Most often, the type of facility for SAQ B merchants is limited to “Office or Departmental Setting”, “Front Desk”, or “Cashier Office” as your process involves dial-up or cellular swipe terminals. |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| Part 2d. Payment Application(s) | Payment Applications are systems or software that are:  
- Hosted and managed by the University, and  
- Used to store, process, or transmit cardholder data electronically.  
An example of a Payment Application is a Point of Sale system.  
Most often, for SAQ B merchants, there are no payment applications being used as you are processing payments through the use of a stand-alone payment terminal. |
| Part 2e. Description of Environment | “Provide a high-level description of the environment covered by this assessment.”  
Most often, a high-level description of an SAQ B environment is limited to a statement such as “For payment card transactions, the department uses a standalone dial-up swipe terminal connected via a phone line to Wells Fargo Merchant Services”.  
“Does your business use network segmentation to affect the scope of your PCI DSS environment?”  
For SAQ B merchants, payment card transactions are not transmitted using the University’s network, so the answer to this question should be “No”. |
| Part 2f. Third-Party Service Providers | “Does your company use a Qualified Integrator & Reseller (QIR)?”  
For SAQ B merchants, you most likely do not use a Qualified Integrator and Reseller Company (QIR Company) to implement, configure, and/or support your payment card environment, so the answer to this question would be “No”.  
“Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment |
A third-party service provider is any company that stores, transmits, or processes payment cards for the University; or any entity that can affect the security of cardholder data.

Examples of third-party service providers include Authorize.net, AudienceView, Active Networks, Amazon Web Services, PayPal, RegOnline, and others.

Make sure to list all third-party service providers that your area uses to store, transmit, or process payment cards.

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Eligibility to Complete SAQ B

Carefully read each of the four statements. Note the first box includes two statements joined by “and/or”. As long as one statement is true for your account you may check the box. Check each statement that is true for your account. If any statements are not true for your account, or if you are unsure, contact Accounts Receivable Services at pmtcard@umn.edu.

Section 2: Self-Assessment Questionnaire

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

*University of Minnesota SAQ-B accounts typically answer each question in this section “Yes”.*

However, a common finding by outside assessors is the lack of written procedures that document how a merchant complies with specific PCI DSS requirements, such as Requirement 3. The University maintains written information security policies that apply to merchant accounts. However, each merchant must create and maintain written operational procedures that reference broader University policies and detail day-to-day practices associated with the merchant account. Procedures can be brief and may be incorporated into other written procedures in the unit.

Below are examples of common operational procedures for Requirement 3 questions for SAQ-B accounts. You may add to and customize these to develop the procedures that apply to your practices. Operational procedures are not included with the SAQ, but are used to train unit employees, and must be readily available.
available to share on request. As such, all written documents relating to your merchant account(s) should be placed in the CampusGuard Document Locker provided with your portal account. THESE ARE EXAMPLES. THE PROCEDURES DESCRIBED MAY NOT BE APPLICABLE TO YOUR AREA. THE GOAL IS TO DOCUMENT EACH STEP IN THE ACCEPTANCE OF PAYMENT CARDS FOR YOUR ACCOUNT, AS THOUGH WRITING THEM FOR A NEW EMPLOYEE.

1. **Phone payments**  “When accepting a customer’s payment card information over the phone, the merchant manager [or his/her designee] writes the card information on a piece of paper, immediately enters the data into the swipe terminal, and immediately shreds the paper in a cross-cut shredder. If the merchant manager is unable to immediately enter the data and shred the paper, the paper containing cardholder data is placed in a locked cabinet, drawer, or safe to which only the merchant manager and a designee have access.”

2. **Display of card numbers in accounting system**  “Only the last 4 digits of card numbers are displayed in systems used to reconcile accounts.” [Note: The last 4 digits of card numbers alone do not constitute “cardholder data”, and thus the systems storing this data are out of scope for PCI DSS.]

3. **What to do if cardholder data is received via email**  “Cardholder information may not be received through email. In the rare case that a customer emails their cardholder data to the department, delete the email, empty your recycle bin, follow other procedures as recommended by University Information Security, contact the customer immediately via a separate email or by phone to explain that the University may not accept card information via an email for security reasons, and describe their available options.”

4. **Paper-based remittance forms**  “Paper-based remittance forms are designed with a tear-off portion for the customer’s card data which can be torn off and shredded immediately after processing. Mailed-in invoices are received, opened, and processed by the merchant manager [or his/her designee] the day they are received or as soon as possible. Unprocessed invoices and unopened mail expected to contain customer payment data are kept in a secure area such as a safe or locked file that is only accessible by the merchant manager or a designee.”

<p>| Requirement 4: Encrypt transmission of cardholder data across open, public networks |
| Requirement 4.2 (b) Are policies in place that state unprotected PANs are not to be sent via end-user messaging technologies? |
| Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments. Although this is covered at a high level by University data security and privacy policies, add a statement to your operational procedures to reflect compliance with this item (see #3 under Requirement 3 above “What to do if cardholder data is received via email”). |</p>
<table>
<thead>
<tr>
<th>Requirement 7: Restrict access to cardholder data by business need to know</th>
<th>To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job. You can typically answer “Yes” to this question if you limit access to your swipe terminal(s) and cardholder data (paper forms or the actual card as shared in person by the card holder) to only those individuals whose jobs require access; for example, the Payment Card Manager and cashiers. If your area does not limit access to your swipe terminal(s) and cardholder data to only those individuals with a business need, contact the Payment Card Program at <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> to discuss your process. Note: Reports used for account reconciliation that only list the last 4 digits of a card number do not constitute cardholder data for PCI DSS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 9: Restrict physical access to cardholder data</td>
<td>Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data. Two common findings are (1) the need to recognize where increased security is required, and (2) to document all operational procedures in writing.</td>
</tr>
<tr>
<td>9.5 Are all media physically secured? (media includes computers, removable electronic media, hard drives, portable drives, USB sticks, CDs, DVDs, paper reports, paper receipts, and faxes)</td>
<td>If your area accepts credit card payments via telephone, fax, or mail, you most likely receive cardholder data written on paper. These paper documents with cardholder data have to be securely handled, such as keeping them in locked storage at all times other than when being processed.</td>
</tr>
<tr>
<td>Section</td>
<td>Question</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>9.6 (a)</td>
<td>Is strict control maintained over the internal or external distribution of any kind of media?</td>
</tr>
<tr>
<td>9.6 (b)</td>
<td>Do controls include the following: 9.6.1 Is media classified so the sensitivity of the data can be determined? 9.6.2 Is media sent by secured courier or other delivery method that can be accurately tracked? 9.6.3 Is management approval obtained prior to moving the media?</td>
</tr>
<tr>
<td>9.7</td>
<td>Is strict control maintained over the storage and accessibility of media?</td>
</tr>
<tr>
<td>9.8 (a)</td>
<td>Is all media destroyed when it is no longer needed for business or legal reasons? 9.8 (c) Is media destruction performed as follows: 9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? 9.8.1 (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?</td>
</tr>
<tr>
<td>9.9</td>
<td>Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows? 9.9 (a) Do policies and procedures require that a list of such devices maintained? 9.9 (b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?</td>
</tr>
<tr>
<td>9.9 (c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>
| **9.9.1 (a)** Does the list of devices include the following?  
- Make, model of device  
- Location of device  
- Device serial number  
**9.9.1 (b)** Is the list accurate and up to date?  
**9.9.1 (c)** Is the list of devices updated when devices are added, relocated, decommissioned, etc.? |
| Maintaining a Payment Card Inventory List and reviewing and uploading this list to the CampusGuard Document Locker annually would typically address these questions. |

| 9.9.2 (a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?  
9.9.2 (b) Are personnel aware of procedures for inspecting devices? |
|---|
| Ensuring that your procedures include inspecting your swipe terminal upon use, and reporting possible tampering (unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings), would typically address these questions.  
**All employees responsible for processing payment card transactions using your payment card terminal(s) should also be aware of this requirement.** |

| 9.9.3 Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?  
9.9.3 (a) Do training materials for personnel at point-of-sale locations include the following?  
- Verify the identity of any third party persons claiming to be repair or maintenance personnel.  
- Do not install, replace, or return devices without verification.  
- Be aware of suspicious behavior around devices.  
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel.  
9.9.3 (b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices? |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring that your procedures include inspecting your swipe terminal upon use, and reporting possible tampering (unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings), would typically address these questions.</td>
</tr>
</tbody>
</table>
**Requirement 12: Maintain a policy that addresses information security for all personnel**

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity's site or otherwise have access to the cardholder data environment.

A common concern in this area is ensuring that merchants maintain adequate payment card procedures which include explanations on employee training and termination, how customers pay for purchases, disposal of cardholder data, and incident response.

*Note: Each merchant must have a written statement in their operational procedures stating they comply with University of Minnesota Information Security Policies and Procedures.*

<table>
<thead>
<tr>
<th>12.1 Is a security policy established, published, maintained, and disseminated to all relevant personnel?</th>
<th>If you maintain and annually review a “Department Payment Card Operational Procedures” document you are able to answer “Yes” to this question. Keep in mind that this “Payment Card Operational Procedures” document has to be uploaded to the CampusGuard Document Locker annually as well.</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1.1 Is the security policy reviewed at least annually and updated when the environment changes?</td>
<td>If you maintain and annually review a “Department Payment Card Operational Procedures” document can typically answer “Yes” to this question. Keep in mind that this “Payment Card Operational Procedures” document has to be uploaded to the CampusGuard Document Locker annually as well.</td>
</tr>
<tr>
<td>12.3 Are usage policies for critical technologies developed to define proper use of these technologies and require the following:</td>
<td>The University maintains authorization approval policies for critical technologies. If you maintain language in your Payment Card Operational Procedures talking about who has authorization to use your critical technologies (ex. swipe terminal is only to be used by the Payment Card Manager and employees who have been appropriately trained and signed a UM1623 form, etc.), you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.</td>
<td>12.3.1 Explicit approval by authorized parties to use the technologies?</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.3.3 A list of all such devices and personnel with access?</td>
<td>The University maintains a list of all critical devices and those authorized to access these devices. If you maintain a “Payment Card Inventory List” and ensure that employees with access to your critical technologies are trained and documented, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.3.5 Acceptable uses of the technologies?</td>
<td>The University maintains authorization approval policies for critical technologies. If you maintain language in your Payment Card Operational Procedures talking about the acceptable uses of any critical technologies (ex. wireless access not allowed for payment processing, employees not allowed to process payments using their work computer, etc.), you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.4 Do security policy and procedures clearly define information security responsibilities for all personnel?</td>
<td>The University maintains security policies and procedures which define security responsibilities for all personnel. If you maintain language in your Payment Card Operating Procedures talking about the importance of payment card security as well as who is responsible for ensuring this security, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.5 (b) Are the following information security management responsibilities formally assigned to an individual or team:</td>
<td>The University maintains a security incident response team to ensure timely and effective handling of all situations. If you maintain and annually review the UM1634 Form “Incident Response and Continuity Plan”, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.5.3 Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?</td>
<td></td>
</tr>
<tr>
<td>12.6 (a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?</td>
<td>The University maintains a formal security awareness program. If you have completed all assigned training videos and training workshops and have instituted and maintain a payment card training program for your employees, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:</td>
<td>Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked “Not Applicable (N/A)” (with a corresponding statement such as “Data is not shared with service providers” in Appendix C: Explanation of Non-Applicability.</td>
</tr>
<tr>
<td>12.8.1 Is a list of service providers maintained?</td>
<td>Note: A third-party service provider is any company that stores, transmits, or processes payment cards for the University, as well as any company that could affect the security of a</td>
</tr>
</tbody>
</table>
Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, and others.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.8.2</td>
<td>Is a written agreement maintained that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess? Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked “Not Applicable (N/A)” (with a corresponding statement such as “Data is not shared with service providers” in Appendix C: Explanation of Non-Applicability.</td>
</tr>
<tr>
<td>12.8.3</td>
<td>Is there an established process for engaging service providers, including proper due diligence prior to engagement? Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked “Not Applicable (N/A)” (with a corresponding statement such as “Data is not shared with service providers” in Appendix C: Explanation of Non-Applicability.</td>
</tr>
<tr>
<td>12.8.4</td>
<td>Is a program maintained to monitor service providers’ PCI DSS compliance status? Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked “Not Applicable (N/A)” (with a corresponding statement such as “Data is not shared with service providers” in Appendix C: Explanation of Non-Applicability.</td>
</tr>
<tr>
<td>12.8.5</td>
<td>Is information maintained about which PCI DSS requirements are managed by each service provider? Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked “Not Applicable (N/A)” (with a corresponding statement such as “Data is not shared with service providers” in Appendix C: Explanation of Non-Applicability.</td>
</tr>
<tr>
<td>12.10.1</td>
<td>(a) Has an incident response plan been created to be implemented in the event of system breach? If you maintain and annually review the UM1634 Form “Incident Response and Continuity Plan”, you can typically answer “Yes” to this question. Keep in mind that this form has to be uploaded to the CampusGuard Document Locker annually as well.</td>
</tr>
</tbody>
</table>
### Appendix B: Compensating Controls Worksheet

**Compensating Controls Worksheet**

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

Compensating controls must:

1. Meet the intent and rigor of the original stated PCI DSS requirement;
2. Provide a similar level of defense as the original PCI DSS requirement;
3. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

If you answered “Compensating Control Used” to any of the questions shown in the requirement sections, contact pmtcard@umn.edu for further guidance on how to complete this section.

Typically, merchants do not use compensating controls, so this section can be left blank.

### Appendix C: Explanation of Non-Applicability

**Explanation of Non-Applicability**

If you answered “Not Applicable (N/A)” to any of the questions shown in the requirement sections, you are required to use this worksheet to explain why the related requirement is not applicable to your area.

### Section 3: Validation and Attestation Details

**Part 3. PCI DSS Validation**

After completing the body of the SAQ, if you answered “Yes” or “Not Applicable (N/A)” to all the questions asked in the requirements sections, your area is compliant and you can check the “Compliant” box.

If you answered “No” to any of the questions asked in the requirements sections, your area is non-compliant, and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section.

Typically, “Compliant but with Legal Exception” is not checked.
### Part 3a. Acknowledgement of Status

After completing the body of the SAQ, carefully read each of the statements shown in this section, and check each statement that is true for your account.

- **PCI DSS Self-Assessment Questionnaire B, 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 confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.**  
  *The typical payment system for this SAQ is a dial-up or cellular swipe terminal. Dial-up and cellular swipe terminals do not store sensitive authentication data after authorization.*

- **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 storage after transaction authorization was found on ANY system reviewed during this assessment.**  
  *The typical payment system for this SAQ is a dial-up or cellular swipe terminal. Dial-up and cellular swipe terminals do not store full track data, CAV2, CVC2, CID, CVV2 data, or PIN data after authorization.*

- **ASV scans are being completed by the PCI SSC Approved Scanning Vendor**  
  *As ASV scans are not required for dial-up or cellular payment terminals you should be able to leave this question blank.*

If you are unsure about any of the questions shown in this section, contact the Payment Card Program at pmtcard@umn.edu.
<table>
<thead>
<tr>
<th>Part 3b. Merchant Attestation</th>
<th>After completing the body of the SAQ the Payment Card Manager is to type in the current date, and enter their name and title as the “Merchant Executive Officer”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 3c. QSA Acknowledgement (if applicable)</td>
<td>This section does not need to be completed.</td>
</tr>
<tr>
<td>Part 3d. ISA Acknowledgement (if applicable)</td>
<td>This section does not need to be completed.</td>
</tr>
</tbody>
</table>
| Part 4. Action Plan for Non-Compliant Status | This section is a summary of the PCI DSS requirements shown in your questionnaire. If you answered “Yes” or “Not Applicable (N/A)” to all the questions asked in the requirements sections, your area is compliant and you can check “Yes” for each line item.  

If you answered “No” to any of the questions asked in the requirements sections, your area is non-compliant and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section. |
Self-Assessment Questionnaire (SAQ) P2PE and Attestation of Compliance Guidance

The intent of this guidance is to assist University of Minnesota Payment Card Managers in completing their annual PCI DSS Self-Assessment Questionnaire (SAQ) and Attestation of Compliance. Specifically, this document is for use with accounts that qualify to complete an SAQ B (see description below). 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 P2PE

SAQ Description: 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. The SAQ P2PE SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a validated P2PE hardware device.

SAQ P2PE merchants confirm that, for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC;
- The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution;
- Your company does not otherwise receive or transmit cardholder data electronically;
- There is no legacy storage of electronic cardholder data in the environment;
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Your company has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

This SAQ is not applicable to e-commerce channels.

All merchants must comply with all twelve requirements of the Payment Card Industry Data Security Standards (PCI DSS). However, the self-assessment for SAQ B merchants focuses on portions of five standards:

Requirement 3: Protect stored cardholder data

Requirement 9: Restrict physical access to cardholder data
**Requirement 12: Maintain a policy that addresses information security for all personnel**

**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) for your account(s). This electronic SAQ allows you to complete your questionnaire online. You can access your CampusGuard Portal by logging in at [http://portal.campusguard.com/loginso](http://portal.campusguard.com/loginso).

For each question, there is a choice of responses to indicate your area’s status regarding that requirement. **Only one response should be selected for each question.** A description of the meaning for each response is provided in the table below.

<table>
<thead>
<tr>
<th>Response</th>
<th>When to use this response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>The expected testing has been performed, and all elements of the requirement have been met as stated.</td>
</tr>
<tr>
<td>No</td>
<td>Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.</td>
</tr>
<tr>
<td></td>
<td>Selecting this response would mean your area is not compliant with PCI DSS requirements.</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>If you do not know the answer to the requirement, contact <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> for guidance prior to selecting this response.</td>
</tr>
<tr>
<td></td>
<td>Selecting this response would mean your area is not compliant with PCI DSS requirements.</td>
</tr>
<tr>
<td>Not Applicable (N/A)</td>
<td>The requirement does not apply to the environment.</td>
</tr>
<tr>
<td></td>
<td>All responses in this column require a supporting explanation in Appendix C of the SAQ.</td>
</tr>
<tr>
<td>Compensating Control Used</td>
<td>The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.</td>
</tr>
<tr>
<td></td>
<td>As all responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ, contact <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a> for guidance prior to selecting this response.</td>
</tr>
</tbody>
</table>
**Guidance for Completing Your SAQ:** The following chart offers guidance and helpful hints, which may be useful as you are completing your Self-Assessment Questionnaire.

<table>
<thead>
<tr>
<th>Section 1: Assessment Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAQ Section or Question</strong></td>
<td><strong>Helpful Hints &amp; Common Findings</strong></td>
</tr>
</tbody>
</table>
| **Merchant and Qualified Security Assessor Information** | Complete this section with the contact information for your merchant area/department including the contact information for the merchant manager who has responsibility for the merchant account and the payment card activities in the office.  
**Note:** Company Name should be “Regents of the University of Minnesota”, and DBA (doing business as) should be your Payment Card Account Name. |
| Part 1a. Merchant Organization Information | Part 1b. Qualified Security Assessor Company Information (if applicable) | Since the University rolls our SAQs up into a single report to submit to our acquiring bank you can leave this section blank. |
| **Executive Summary**             | **Select the type of business that is applicable to your area or department.**  
**Check the types of credit and debit card payment channels that your area uses.**  
**Check the types of payment channels that are covered by this SAQ. Most often, this is limited to “Card-present (face-to-face)” and at times “MOTO” for SAQ P2PE merchants. This SAQ is not to be used for “E-Commerce” payment methods. If your area accepts payment cards online, you will need to complete an SAQ A, as well.** |
| Part 2a. Type of Merchant Business (check all that apply) | Part 2b. Description of Payment Card Business | Describe your payment card environment in detail. Be sure to include an explanation of:  
- **What the customer is purchasing,**  
- **How you process credit card payments (your payment card environment), and**  
- **Any service provider(s) and how they interact with your payment card environment.**  
- **If you store payment card information electronically or on paper, explain how and why this is done.**  
An example description may be, “The department has a merchant account using a P2PE provider which allows us to accept in-person and MOTO credit and debit card payments.” |
| Part 2c. Locations | Describe the type of facility included in your PCI DSS review.  
| | Most often, the type of facility for SAQ P2PE merchants is limited to “Office or Departmental Setting”, “Front Desk”, or “Cashier Office” as your process involves P2PE payment card terminals. |
| Part 2d. P2PE Solution | “Provide the following information regarding the validated PCI P2PE solution your organization uses:”  
| | Name of P2PE Solution Provider:  
| | This is the name of the company that you contracted with to provide P2PE services. Common P2PE providers include Bluefin, FreedomPay, and CardConnect. A list of all P2PE providers can be found at [PCI SSC - Validated P2PE Solutions](#)  
| | Name of P2PE Solution:  
| | This is the name of the solution provided by the P2PE Solution Provider shown above. A list of all P2PE providers and solutions can be found at [PCI SSC - Validated P2PE Solutions](#)  
| | PCI SSC Reference Number:  
| | This is the reference number for the P2PE Solution shown above. A list of all P2PE Solutions and Reference Numbers can be found at [PCI SSC - Validated P2PE Solutions](#)  
| | Listed P2PE POI Devices used by Merchant (PTS Device Dependencies):  
| | This is the make and model of the P2PE payment card terminal that your area is using. Common P2PE POI devices include IDTech SREDKey, Ingenico iCT220, Ingenico iCT250, Ingenico iSC250 Touch, etc. A list of all P2PE Solution Dependencies can be found at [PCI SSC - Validated P2PE Solutions](#)  
| Part 2e. Description of Environment | “Provide a high-level description of the environment covered by this assessment.”  
| | Most often, a high-level description of an SAQ P2PE environment is limited to a statement such as “For payment card transactions, the department uses a P2PE payment card terminal connected via USB to a POS system. The P2PE terminal interacts with a validated P2PE
provider. Funding is provided to the University through the use of a University merchant account.

“Does your business use network segmentation to affect the scope of your PCI DSS environment?”

For SAQ P2PE merchants, payment card transactions are encrypted prior to accessing the University network, so network segmentation is not required. As such, the answer to this question should be “No”.

<table>
<thead>
<tr>
<th>Part 2f. Third-Party Service Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Does your company use a Qualified Integrator &amp; Reseller (QIR)?”</td>
</tr>
<tr>
<td>If your area uses a vendor to implement, configure, and/or support your P2PE payment card terminals, this vendor must be a Qualified Integrator and Reseller Company (QIR Company) as they have access to the cardholder environment.</td>
</tr>
<tr>
<td>“Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator &amp; Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?”</td>
</tr>
<tr>
<td>A third-party service provider is any company that stores, transmits, or processes payment cards for the University; or any entity that can affect the security of cardholder data.</td>
</tr>
<tr>
<td>Examples of third-party service providers within a P2PE environment include the P2PE provider, such as Bluefin, FreedomPay, CardConnect, etc.</td>
</tr>
<tr>
<td>Make sure to list all third-party service providers that your area uses to store, transmit, or process payment cards.</td>
</tr>
<tr>
<td>Note: Requirement 12.8 applies to all entities in this list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2g. Eligibility to Complete SAQ P2PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carefully read each of the six statements. Check each statement that is true for your account. If any statements are not true for your account, or if you are unsure, contact Accounts Receivable Services at <a href="mailto:pmtcard@umn.edu">pmtcard@umn.edu</a>.</td>
</tr>
</tbody>
</table>
Section 2: Self-Assessment Questionnaire

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

If your area does not accept MOTO payments, you should be able to answer each question in this section as “N/A” because you do not have cardholder data stored electronically or on paper.

If your area accepts credit card payment via mail and telephone (MOTO) and store this paperwork, you should be following all of these requirements and answering the questions with a “Yes” response.

A common finding by outside assessors is the lack of written procedures that document how a merchant complies with specific PCI DSS requirements, such as Requirement 3. The University maintains written information security policies that apply to merchant accounts. However, each merchant must create and maintain written operational procedures that reference broader University policies and detail day-to-day practices associated with the merchant account. Procedures can be brief and may be incorporated into other written procedures in the unit.

Below are examples of common operational procedures for Requirement 3 questions for SAQ P2PE accounts. You may add to and customize these to develop the procedures that apply to your practices. Operational procedures are not included with the SAQ, but are used to train unit employees, and must be readily available to share on request. As such, all written documents relating to your merchant account(s) should be placed in the CampusGuard Document Locker provided with your portal account. THESE ARE EXAMPLES. THE PROCEDURES DESCRIBED MAY NOT BE APPLICABLE TO YOUR AREA. THE GOAL IS TO DOCUMENT EACH STEP IN THE ACCEPTANCE OF PAYMENT CARDS FOR YOUR ACCOUNT, AS THOUGH WRITING THEM FOR A NEW EMPLOYEE.

5. **Phone payments** “When accepting a customer’s payment card information over the phone, the merchant manager [or his/her designee] writes the card information on a piece of paper, immediately enters the data into the swipe terminal, and immediately shreds the paper in a cross-cut shredder. If the merchant manager is unable to immediately enter the data and shred the paper, the paper containing cardholder data is placed in a locked cabinet, drawer, or safe to which only the merchant manager and a designee have access.”

6. **Display of card numbers in accounting system** “Only the last 4 digits of card numbers are displayed in systems used to reconcile accounts.” [Note: The last 4 digits of card numbers alone do not constitute “cardholder data”, and thus the systems storing this data are out of scope for PCI DSS.]

7. **What to do if cardholder data is received via email** “Cardholder information may not be received through email. In the rare case that a customer emails their cardholder data to the department, delete the email, empty your recycle bin, follow other procedures as recommended by University Information Security, contact the customer immediately via a separate email or by phone to explain...”
8. **Paper-based remittance forms** “Paper-based remittance forms are designed with a tear-off portion for the customer’s card data which can be torn off and shredded immediately after processing. Mailed-in invoices are received, opened, and processed by the merchant manager [or his/her designee] the day they are received or as soon as possible. Unprocessed invoices and unopened mail expected to contain customer payment data are kept in a secure area such as a safe or locked file that is only accessible by the merchant manager or a designee.”

| Requirement 9: Restrict physical access to cardholder data | Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

Two common findings are (1) the need to recognize where increased security is required, and (2) to document all operational procedures in writing.

| 9.5 Are all media physically secured? (media includes computers, removable electronic media, hard drives, portable drives, USB sticks, CDs, DVDs, paper reports, paper receipts, and faxes) | If your area accepts credit card payments via telephone, fax, or mail, you most likely receive cardholder data written on paper. These paper documents with cardholder data have to be securely handled, such as keeping them in locked storage at all times other than when being processed.

| 9.8 (a) Is all media destroyed when it is no longer needed for business or legal reasons? | In this context, the destruction of media refers to cross-cut shredding any paper with cardholder data immediately after processing.

**The University does not recommend using storage containers for the disposal of cardholder data after processing.**

<p>| 9.8 (c) Is media destruction performed as follows: 9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? 9.8.1 (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents? |</p>
<table>
<thead>
<tr>
<th>9.9 Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?</th>
<th>9.9 (a) Completing and uploading your Payment Card Inventory List to the CampusGuard Document Locker would typically address this question.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9 (a) Do policies and procedures require that a list of such devices maintained?</td>
<td>9.9 (b) and 9.9 (c) Your procedures should include inspecting your swipe terminal for tampering and substitution upon use, and reporting any suspicious behavior or possible tampering to <a href="mailto:abuse@umn.edu">abuse@umn.edu</a>.</td>
</tr>
<tr>
<td>9.9 (b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?</td>
<td></td>
</tr>
<tr>
<td>9.9 (c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?</td>
<td></td>
</tr>
</tbody>
</table>

9.9.1 (a) Does the list of devices include the following?
- Make, model of device
- Location of device
- Device serial number

9.9.1 (b) Is the list accurate and up to date?
9.9.1 (c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?

9.9.2 (a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?

9.9.2 (b) Are personnel aware of procedures for inspecting devices?

9.9.3 Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?
9.9.3 (a) Do training materials for personnel at point-of-sale locations include the following?
- Verify the identity of any third party persons claiming to be repair or maintenance personnel.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices.
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel.

9.9.3 (b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?

<table>
<thead>
<tr>
<th>9.10 Are security policies and operational procedures for restricting physical access to cardholder data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Documented</td>
</tr>
<tr>
<td>• In use</td>
</tr>
<tr>
<td>• Known to all affected parties?</td>
</tr>
</tbody>
</table>

A "Yes" answer to Requirement 9.10 means that your area has policies and procedures in place for Requirements 9.5, 9.8, and 9.9, as applicable for your environment. This helps to ensure personnel are aware of and following security policies and documented operational procedures.

**Requirement 12: Maintain a policy that addresses information security for all personnel**

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

A common concern in this area is ensuring that merchants maintain adequate payment card procedures which include explanations on employee training and termination, how customers pay for purchases, disposal of cardholder data, and incident response.

*Note: Each merchant must have a written statement in their operational procedures stating they comply with University of Minnesota Information Security Policies and Procedures.*

| 12.1 Is a security policy established, published, maintained, and disseminated to all relevant personnel? |

If you maintain and annually review a “Department Payment Card Operational Procedures” document you are able to answer “Yes” to this question. Keep in mind that this “Payment Card Operational Procedures” document has to be uploaded to the CampusGuard Document Locker annually as well.

| 12.1.1 Is the security policy reviewed at least annually and updated when the environment changes? |

If you maintain and annually review a “Department Payment Card Operational Procedures” document can typically answer “Yes” to this question. Keep in mind that this “Payment Card Operational Procedures” document has to be uploaded to the CampusGuard Document Locker annually as well.
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4 Do security policy and procedures clearly define information security responsibilities for all personnel?</td>
<td>The University maintains security policies and procedures which define security responsibilities for all personnel. If you maintain language in your Payment Card Operating Procedures talking about the importance of payment card security as well as who is responsible for ensuring this security, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.5 Are the following information security management responsibilities formally assigned to an individual or team: 12.5.3 Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?</td>
<td>The University maintains a security incident response team to ensure timely and effective handling of all situations. If you maintain and annually review the UM1634 Form “Incident Response and Continuity Plan”, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.6 (a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?</td>
<td>The University maintains a formal security awareness program. If you have completed all assigned training videos and training workshops and have instituted and maintain a payment card training program for your employees, you can typically answer “Yes” to this question.</td>
</tr>
<tr>
<td>12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: 12.8.1 Is a list of service providers maintained?</td>
<td>As SAQ P2PE accounts requires at least the use of a P2PE Provider, your process involves at least one third party service provider supplying the P2PE payment gateway which processes the credit card payments entered into the P2PE POI devices. Examples of third-party service providers include Bluefin, FreedomPay, CardConnect, and others. The answer to this question should be “Yes”, as the Accounts Receivable Services department maintains a list of service providers.</td>
</tr>
<tr>
<td>Note: A third-party service provider is any company that stores, transmits, or processes payment cards for the University, as well as any company that could affect the security of a cardholder transaction. Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, and others.</td>
<td>12.8.2 Is a written agreement maintained that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess? As SAQ P2PE accounts requires at least the use of a P2PE Provider, your process involves at least one third party service provider supplying the P2PE payment gateway which processes the credit card payments entered into the P2PE POI devices. Examples of third-party service providers include Bluefin, FreedomPay, CardConnect, and others.</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?</td>
<td>As SAQ P2PE accounts requires at least the use of a P2PE Provider, your process involves at least one third party service provider supplying the P2PE payment gateway which processes the credit card payments entered into the P2PE POI devices. Examples of third-party service providers include Bluefin, FreedomPay, CardConnect, and others. The answer to this question should be “Yes”, as the Accounts Receivable Services department maintains an established process for engaging service providers.</td>
</tr>
<tr>
<td>12.8.4 Is a program maintained to monitor service providers’ PCI DSS compliance status?</td>
<td>As SAQ P2PE accounts requires at least the use of a P2PE Provider, your process involves at least one third party service provider supplying the P2PE payment gateway which processes the credit card payments entered into the P2PE POI devices. Examples of third-party service providers include Bluefin, FreedomPay, CardConnect, and others. The answer to this question should be “Yes”, as the Accounts Receivable Services department maintains a program to monitor the PCI DSS compliance status of all service providers.</td>
</tr>
<tr>
<td>12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider?</td>
<td>As SAQ P2PE accounts requires at least the use of a P2PE Provider, your process involves at least one third party service provider supplying the P2PE payment gateway which processes the credit card payments entered into the P2PE POI devices. Examples of third-party service providers include Bluefin, FreedomPay, CardConnect, and others. The answer to this question should be “Yes”, as the Accounts Receivable Services department maintains information about which PCI DSS requirements are managed by each service provider.</td>
</tr>
<tr>
<td>12.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?</td>
<td>If you maintain and annually review the UM1634 Form &quot;Incident Response and Continuity Plan&quot;, you can typically answer “Yes” to this question. Keep in mind that this form...</td>
</tr>
</tbody>
</table>
has to be uploaded to the CampusGuard Document Locker annually as well.

**Appendix B: Compensating Controls Worksheet**

| Compensating Controls Worksheet | Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:
1) Meet the intent and rigor of the original stated PCI DSS requirement;
2) Provide a similar level of defense as the original PCI DSS requirement;
3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

If you answered “Compensating Control Used” to any of the questions shown in the requirement sections, contact pmtcard@umn.edu for further guidance on how to complete this section.

Typically, merchants do not use compensating controls, so this section can be left blank.

**Appendix C: Explanation of Non-Applicability**

| Explanation of Non-Applicability | If you answered “Not Applicable (N/A)” to any of the questions shown in the requirement sections, you are required to use this worksheet to explain why the related requirement is not applicable to your area.

**Section 3: Validation and Attestation Details**

| Part 3. PCI DSS Validation | After completing the body of the SAQ, if you answered “Yes” or “Not Applicable (N/A)” to all the questions asked in the requirements sections, your area is compliant and you can check the “Compliant” box.

If you answered “No” to any of the questions asked in the requirements sections, your area is non-compliant, and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section.
<table>
<thead>
<tr>
<th>Part 3a. Acknowledgement of Status</th>
<th>Typically, “Compliant but with Legal Exception” is not checked.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>After completing the body of the SAQ carefully read each of the statements shown in this section, and check each statement that is true for your account.</td>
</tr>
<tr>
<td></td>
<td>• <em>PCI DSS Self-Assessment Questionnaire SAQ P2PE, Version 3.2.1,</em> was completed according to the instructions therein.</td>
</tr>
<tr>
<td></td>
<td>• All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.</td>
</tr>
<tr>
<td></td>
<td>• I have read the <em>PCI DSS</em> and I recognize that I must maintain <em>PCI DSS</em> compliance, as applicable to my environment, at all times.</td>
</tr>
<tr>
<td></td>
<td>• If my environment changes, I recognize I must reassess my environment and implement any additional <em>PCI DSS</em> requirements that apply.</td>
</tr>
</tbody>
</table>
|                                   | • No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment.  
  The typical payment system for this SAQ is a dial-up or cellular swipe terminal.  Dial-up and cellular swipe terminals do not store full track data, CAV2, CVC2, CID, CVV2 data, or PIN data after authorization. |
|                                   | If you are unsure about any of the questions shown in this section, contact the Payment Card Program at pmtn@umn.edu. |
| Part 3b. Merchant Attestation     | After completing the body of the SAQ the Payment Card Manager is to type in the current date, and enter their name and title as the “Merchant Executive Officer”. |
| Part 3c. QSA Acknowledgement (if applicable) | **This section does not need to be completed.** |
| Part 3d. ISA Involvement (if applicable) | **This section does not need to be completed.** |
| Part 4. Action Plan for Non-Compliant Requirements | This section is a summary of the *PCI DSS* requirements shown in your questionnaire. If you answered “Yes” or |
“Not Applicable (N/A)” to all the questions asked in the requirements sections, your area is compliant and you can check “Yes” for each line item.

If you answered “No” to any of the questions asked in the requirements sections, your area is non-compliant and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section.
SAQ Frequently Asked Questions

Q: If I am the Payment Card Manager of multiple accounts, will I have to complete multiple SAQs?

A: Yes. If you are the Payment Card Manager responsible for multiple accounts with different payment processes (online, terminal, POS, etc.), each of your distinct processes have been assigned a different SAQ. The SAQs assigned to you in the portal are the SAQs which includes all the questions you must answer for all the accounts you are responsible for. For example, if you are responsible for one swipe terminal account and one online account, you will need to complete an SAQ B for your swipe terminal process, and an SAQ A for your online process. Keep in mind there may be exceptions to this rule, so contact Accounts Receivable Services at pmtcard@umn.edu if you have any questions.

Q: When I log into the CampusGuard Portal to complete my SAQ(s), all I see is last year’s SAQ. How should I complete this year’s SAQ(s)?

A: When you log into the CampusGuard Portal, you should see the SAQ (or SAQs) that you are responsible to complete. If the SAQ has been completed in the past, you will click on the “Continue” button to start completing your SAQ. If the SAQ has not been completed in the past, or this is a new version of the SAQ, you will click on the “Start” button to start completing your SAQ. If the SAQ has been completed in the past, you will need to review the responses to the questions, making sure that these responses are still correct. Make sure you read all the questions, keeping in mind that any changes to your payment card environment could now affect the answers to these questions. Contact Accounts Receivable Services at pmtcard@umn.edu if you have any questions on how to complete your SAQ.

Q: Are there any documents out there that can help me complete my SAQ?

A: To help you complete your SAQ(s), there are many documents available for your reference:

- The Payment Card Industry Security Standards Council (PCI SSC) website has a helpful document titled the “Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire Instructions and Guidelines”. This document can be found in the PCI SSC Document Library at https://www.pcisecuritystandards.org/document_library.

- In the General Documents section of the CampusGuard website, you can find a CampusGuard created guidance document to assist you with completion of an SAQ A or SAQ B. This document is titled “CampusGuard – SAQ A and SAQ B – Guidance, Tips, and Common Findings & Responses – PCI DSS v3.2.pdf”.

- If you have specific questions as you complete your SAQ in the CampusGuard portal, you can e-mail CampusGuard using the Request Help (?) icons that are available for each question.
Q: What are the Compliance Documents that I need to complete?

A: To maintain compliance with University policy and PCI DSS, each payment card account has to complete a set of compliance documents upon opening an account and annually thereafter. Below is a listing of the documents that need to be completed. If these documents have been completed in the past, you will need to review each document, ensure they are accurate and up-to-date, and then make sure today’s date is included on the document. Once each of the documents have been completed, they should be uploaded to the CampusGuard Document Locker at: http://portal.campusguard.com/loginssso. To maintain an accurate annual record of your compliance documentation, do not delete your old documents in the CampusGuard Document Locker, and do not save updated documents with the same file name as older documents (as they will overwrite the older documents if they contain the same document file name). Here are the Compliance Documents that need to be completed:

1. **Payment Card Account Department Payment Card Manager Form (UM 1624)**
The Department Payment Card Manager Form is a University form certifying 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).

2. **Payment Card Account Employee Non-Disclosure Form (UM 1623)**
The Employee Non-Disclosure Form is a University form certifying that the signer 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 effort to prevent and protect any part of the cardholder information from disclosure to anyone that does not have a business need for it, and to prevent the release of cardholder information into the public domain or into the possession of unauthorized persons.

3. **Payment Card Account Incident Response and Continuity Plan (UM 1634)**
The Incident Response and Continuity Plan is a document indicating your department’s security incident response plan for security incidents involving payment cards.

4. **Payment Card Operational Procedures**
The Payment Card Operational Procedures document explains the specific payment card transaction process for your area, required training of employees processing payment cards in your area, security of payment card devices in your area, data retention and disposal, and other information pertinent to your area’s payment card processing.

5. **Cardholder Data Flow Chart**
The Cardholder Data Flow Chart is a document showing where payment card data is stored, processed, or transmitted within your environment, as well as identifying all supporting and connected systems and devices.

6. **Payment Card Account Inventory List**
The Payment Card Inventory List is a document listing all payment card devices within your environment. This inventory list should, at a minimum, list the owner, provide contact information, and explain
purpose of the devices. 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.

7. Payment Card Manager Compliance Certification Form

The Payment Card Manager Compliance Certification Form is a checklist certifying that the Payment Card Manager has completed all the required annual compliance documents and forms, and that these documents have been uploaded to the CampusGuard Document Locker.

Samples and templates to help you complete your compliance documents can be found on the University’s Payment Card Industry Data Security Standards (PCI DSS) website at http://finsys.umn.edu/business-processes/AR10.html.

Q: I can’t locate a copy of last year’s SAQ and Compliance Documents. Where can I find a copy of these documents?

A: Copies of your SAQ and Compliance Documents from last year should have been saved to your CampusGuard Document Locker.

Q: Do I have to be able to answer YES to every question within the SAQ to be compliant?

A: In order to attest PCI compliance, you must be able to answer YES or N/A to every requirement within the assigned SAQ. The option of Compensating Controls may be considered when a merchant cannot meet a requirement explicitly as stated due to a legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: 1) meet the intent and rigor of the original PCI DSS requirement; 2) Provide a similar level of defense as the original PCI DSS requirement; 3) Be above and beyond the PCI DSS requirements; and 4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. For each compensating control, the merchant must complete a corresponding Compensating Control Worksheet, documenting how the specified control meets the above four criteria, as well as how the control will be maintained. After that worksheet has been prepared, it must be formally accepted by the merchant’s acquirer. Compensating controls are often only approved for a single year with the expectation that the merchant will be able to meet the control as written in the future. A Compensating Control, with permission/approval from your acquiring bank, is acceptable within a compliant SAQ. Unfortunately, one NO answer turns your compliant SAQ into a non-compliant SAQ, however, the priority is always that all questions must be answered honestly and accurately. By partnering with the merchant during SAQ completion process, you should be able to help them successfully remediate any areas identified as non-compliant.

Q: If I answer an SAQ question as “Not Applicable (N/A)”, I think I am supposed to explain why that question is not applicable. How do I do this?
A: For all the questions in your SAQ that you have answered as being “Not Applicable (N/A)”, you are required to explain why that question is not applicable to your process. This explanation can be written in the section of your SAQ titled “Appendix C: Explanation of Non-Applicability”.

Q: If I answer an SAQ question as “No” in my SAQ, does that mean I am not in compliance with PCI DSS?

A: Yes. If you answer a question as “No”, that means your area is not in compliance with that specific PCI DSS requirement. In this instance, you should first contact Accounts Receivable Services (ARS) at pmtcard@umn.edu before you answer the question as “No”.

Q: I don’t understand a question in the SAQ, so is it OK if I answer “Don’t Know”?

A: No. If you don’t understand the question in the SAQ, contact Accounts Receivable Services (ARS) at pmtcard@umn.edu before you answer the question as “Don’t Know”.

Q: What should we provide for the “Description of Payment Card Business” (Part 2b)?

A: Merchants are often unclear as to how much information to provide in this section. CampusGuard recommends providing a high level overview of how cardholder data flows in your business and how (and which) third parties are involved. Part 2b is looking for a description of how payment cards are handled in your environment. Your description should include the processes and procedures for storing, processing, and/or transmitting cardholder data (CHD). Respond to each of the three key areas, for example, "we do not store CHD at any time" and "we use PTS-approved swipe terminals" (consider including the actual terminal type). The response here should give the reader a good idea of how payment cards are handled by the merchant area.

Q: Does the organization use one or more payment applications (Part 2d)?

A: This is another question that is often met with confusion. 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.

Q: Does your business use network segmentation (Part 2e)?

A: You may need to involve IT resources on this question, but basically, network segmentation refers to any physical or logical separation between devices that handle cardholder data and are in PCI scope from those systems that are not in scope for PCI compliance. If there are any firewalls, routers, or other systems in place that restrict network
traffic to or from the systems within the merchant area and between the remainder of the campus network, you would answer “Yes” to this question.

**Q: Who completes and signs off on the SAQ (Part 3b)?**

A: The assigned Payment Card Manager should complete and sign the SAQ for their area(s). It is also acceptable for the area’s Director, Chair, or Dean to sign the SAQ for their area.

**Q: After I’ve completed my SAQ and Compliance Documents, is there anyone that reviews this documentation?**

A: Yes. After you have completed your SAQ and Compliance Documents, they will be reviewed by Accounts Receivable Services (ARS) and University Information Security (UIS). If there are any questions on your documentation, you will be contacted for further clarification.

**Q: After I’ve completed my SAQ, will the SAQ be locked down so I can no longer make changes?**

A: No. The online SAQ in the CampusGuard Portal will not be locked down. This document will remain open and can be updated as needed as the year goes on.

**Q: I need help logging into my CampusGuard Portal. Who can I contact?**

A: If you need assistance logging into the CampusGuard Portal website, please click https://www.campusguard.com/session/help/ to send an e-mail to CampusGuard.

**Q: I am no longer the Payment Card Manager, do I still need to complete the SAQ(s) and Compliance Documents?**

A: If you are no longer the Payment Card Manager on this account, and need to transfer responsibility to a new individual, please contact Accounts Receivable Services at pmtcard@umn.edu.

**Q: We no longer need this payment card account, do I still need to complete the SAQ(s) and Compliance Documents?**

A: If you wish to close a payment card account, please contact Accounts Receivable Services at pmtcard@umn.edu.
Resources

The following are helpful resources relating to payment card policies, procedures, and laws surrounding payment card compliance at the University of Minnesota. If you can't find what you're looking for, contact Accounts Receivable Services at pmtcard@umn.edu for assistance.

- University of Minnesota PCI DSS Compliance
- University Administrative Policy “Accepting Revenue via Payment Cards”
- University of Minnesota Policy “Information Security”
- Payment Card Industry Data Security Standards (PCI DSS)
- Payment Card Industry Security Standards Council (PCI SSC)
- Minnesota Government Data Practices Act
- Minnesota Plastic Card Security Act