Required Documents and Training for Payment Card Managers at the University of Minnesota

As part of the University's dedication to safeguarding our customer's payment card information, units that accept credit or debit cards as a method of payment must meet University policy, follow the Minnesota Government Data Practices Act and Minnesota Plastic Card Security Act, comply with the Payment Card Industry Data Security Standards (PCI DSS), and adhere to our contractual obligations to the University's banks and financial institutions. Links to information on these policies, procedures, and laws can be found at the bottom of this document.

As the Payment Card Manager, you are an integral person in this process. You are the departmental staff person responsible for management of your department's payment card account(s) and must be knowledgeable about the payment card acceptance process in your unit, understand compliance requirements, manage required documentation (such as the PCI DSS Self-Assessment Questionnaire (SAQ) and associated compliance documentation), and be the first point of contact for all questions concerning your payment card account(s). For additional information on the payment card process and your responsibilities as Payment Card Manager visit University Policy "Accepting Revenue via Payment Cards".

Management of your payment card account(s) includes the annual completion of an electronic PCI DSS Self-Assessment Questionnaire (SAQ), associated compliance documentation, and compliance training. Below is an explanation of these requirements:

PCI DSS SELF-ASSESSMENT QUESTIONAIRE (SAQ)

To assist departments and the University with our payment card compliance, there is 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 the CampusGuard website, which includes a Portal for completion of an electronic compliance questionnaire, as well as a Document Locker for the uploading of compliance documentation. The CampusGuard Portal is a secure website containing an electronic version of the appropriate PCI DSS Self-Assessment Questionnaire (SAQ) for your account(s). The CampusGuard Document Locker is a separate area within the CampusGuard website which electronically stores 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 CampusGuard Portal and Document Locker by logging into the CampusGuard website at https://www.campusguard.com/loginsso.

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 the requirements of PCI DSS. Guidance documentation, to assist you with completion of your SAQ(s), can be requested by contacting Accounts Receivable Services at pmtcard@umn.edu. **It is required that this questionnaire be completed upon account activation, and then reviewed and updated annually, or upon any changes to your cardholder data environment.**

COMPLIANCE DOCUMENTS AND FORMS

To maintain compliance with University Policy and PCI DSS, certain payment card compliance documents are to be completed annually and uploaded to the CampusGuard Document Locker. The CampusGuard Document Locker is a separate area within the CampusGuard website which electronically stores 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 CampusGuard Portal and Document Locker by logging into the CampusGuard website at https://www.campusguard.com/loginsso.

It is required that the compliance documents and forms shown below be completed upon merchant account activation, and updated annually or upon any changes to your cardholder data environment:

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

2. **Employee Non-Disclosure Form (UM 1623)**
   The Employee Non-Disclosure Form certifies that the signer of the form has been identified as an employee involved in the payment transaction process who may have access to confidential information related to payment cards. The signer agrees to only use the cardholder information for the intended business purpose of the department; to use their best efforts to prevent and protect any part of the cardholder information from disclosure to the public domain or into the possession of unauthorized persons; that they have read and will abide by associated University policies, laws, and standards; and that they have been trained on the importance of protecting cardholder data. This form can be found in the University Forms Library at http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1623.doc, and should be completed and signed by all employees involved in the payment card process. These forms should then be uploaded to the CampusGuard Document Locker. The Employee Non-Disclosure Form automatically expires at the end of the fiscal year and must be renewed annually.

3. **Incident Response and Continuity Plan (UM 1634)**
   The Incident Response and Continuity Plan details your department's security incident response plan that must be invoked when a security incident involving payment cards has been identified. This form can be found in the University Forms Library at http://policy.umn.edu/sites/policy.umn.edu/files/forms/um1634.doc, and should be completed, signed, and uploaded to the CampusGuard Document Locker upon your assignment as Payment Card Manager. The Incident Response and Continuity Plan automatically expires at the end of the fiscal year and must be renewed annually.
   Note: If this is not a new merchant account, and you are replacing the previous Payment Card Manager, you may be able to update your area's current Incident Response and Continuity Plan, in lieu of creating a new document. A copy of the current Incident Response and Continuity Plan should be found in your CampusGuard Document Locker.

4. **Payment Card Operational Procedures**
   The Payment Card Operational Procedures document explains the specific payment card transaction processes for your area, required training of employees processing payment cards in your area, security of payment card devices in your area, as well as other information pertinent to your area's payment card processing. A template operating procedures document can be found on the University's Payment Card Industry Data Security Standards (PCI DSS) website at http://controller.umn.edu/business-processes/AR10.html. This document should be completed upon your assignment as Payment Card Manager, making sure the template information is updated to reflect your area's specific payment card processes. Once completed, this document should be uploaded to the CampusGuard Document Locker. The Payment Card Operational Procedures document must be reviewed, updated (if needed), re-dated, and uploaded to the CampusGuard Document Locker at the beginning of each fiscal year.
   Note: If this is not a new merchant account, and you are replacing the previous Payment Card Manager, you may be able to review, update (if needed), and re-date your area's current Payment Card Operational Procedures document, in lieu of creating a new document. A copy of the current Payment Card Operational Procedures document should be found in your CampusGuard Document Locker.

5. **Cardholder Data Flow Chart**

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

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

6. **Payment Card Inventory List**

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

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

7. **Payment Card Manager Compliance Certification Form**

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

PAYMENT CARD MANAGER TRAINING

To maintain compliance with University Policy and PCI DSS, Payment Card Managers are required to be **trained upon assignment as a Payment Card Manager, and annually thereafter**. This training consist of the following:

Required Training upon Assignment as a Payment Card Manager

a. View the New Payment Card Manager Training video assigned to you by Accounts Receivable Services. This video provides you with a comprehensive overview of payment card compliance at the University of Minnesota. Reviewing this self-paced video is the first step in your training and should be completed prior to the other training requirements shown below.

b. Complete the Security Awareness Training videos assigned to you by Accounts Receivable Services (ARS). These short videos cover a number of important security topics such as passwords, data security, and PCI DSS. As you

complete each video, you will be required to correctly answer three questions pertaining to the video you just viewed. These videos must be viewed within four weeks of your assignment as Payment Card Manager.

c. Attend the "New Payment Card Manager Meeting" with Accounts Receivable Services (ARS). This meeting is scheduled by Accounts Receivable Services (ARS) upon your assignment as the Payment Card Manager. During this meeting, we will discuss your payment card compliance requirements, tips on how to remain secure in this ever-changing environment, and answer any questions you should have.

Required Training Annually Thereafter

a. Complete the Security Awareness Training videos assigned to you by Accounts Receivable Services (ARS). These short videos cover a number of important security topics such as passwords, data security, and PCI DSS. As you complete each video, you will be required to correctly answer three questions pertaining to the video you just viewed.

b. View the Payment Card Manager Refresher Training video assigned to you by Accounts Receivable Services. This video provides you with an overview of payment card statistics at the University, trends in the security industry, and an in-depth look at the state of payment card security.

OR

Attend one of the in-person "Payment Card Manager Refresher Training" sessions offered by Accounts Receivable Services (ARS). This class provides an overview of payment card statistics at the University, trends in the security industry, and an in-depth look at the state of payment card security. For available sessions, contact Accounts Receivable Services at pmtcard@umn.edu.

HELPFUL LINKS

The following are helpful links 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 Administrative Policy "Accepting Revenue via Payment Cards"
- University Administrative Procedure "Obtaining Approval to Accept Payment Cards"
- University Administrative Procedure "Managing Payment Card Accounts"
- University Administrative Procedure "Requesting Changes to Payment Card Accounts"
- University Administrative Procedure "Closing Payment Card Accounts"
- Minnesota Government Data Practices Act
- Minnesota Plastic Card Security Act
- Payment Card Industry Data Security Standards (PCI DSS)
- Payment Card Industry Security Standards Council (PCI SSC)
- University of Minnesota Payment Card Industry Data Security Standards (PCI DSS)