Required Forms and Documents for Payment Card PCI DSS Compliance

As part of the University’s dedication to safeguarding our customer’s payment card information, there is an annual support agreement in place with CampusGuard to provide resources and expertise needed to achieve and maintain PCI DSS compliance. Included within this agreement is access to the CampusGuard Portal and Document Locker. 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. The CampusGuard Document Locker is a specific area of your portal which electronically stores your critical documents required for PCI DSS compliance. These documents are retained in the portal for reference and verification by your department, Accounts Receivable Services, and CampusGuard.

To access your CampusGuard Portal login at: https://www.campusguard.com/login.

Payment Card Managers are required to complete annually the electronic PCI DSS Self-Assessment Questionnaire (SAQ) shown in the CampusGuard Portal, as well as ensure that current copies of the following documents are uploaded to the CampusGuard Document Locker:

1. **Payment Card Account Department Payment Card Manager Form (UM 1624)**
   The 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. It is required that form UM 1624 be renewed annually.

2. **Hosted Payment Card Account Desktop Usage Agreement (UM 1705) – If applicable**
   The Desktop Usage Agreement is a University form certifying that the payment card manager acknowledges that their unit accesses a University approved on-line, hosted payment gateway website without the need for a secure desktop computer. This hosted payment gateway website is provided by the payment gateway, and allows departments to manage transactions, configure payment gateway account settings, view account statements, and download reports from their desktop computer.

3. **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. It is required that form UM 1623 be renewed annually.

4. **Department Security Incident Response Plan**
   The Department Security Incident Response Plan is a document indicating your department’s security incident response plan for security incidents involving payment cards. It is required that this plan be reviewed, revised, and tested annually. As it is required that this document be reviewed annually, make sure the review date is included on this document.

5. **Operational Procedures**
   Operational Procedures is a document explaining 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 the payment card processing. As it is required that this document be reviewed annually, make sure the review date is included on this document.
6. **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. As it is required that this document be reviewed annually, make sure the review date is included on this document.

7. **Payment Card Inventory List**
   It is required that your area have an inventory list showing 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 a payment processor such as Authorize.net, your inventory list should include information on the University server redirecting the customer to Authorize.net. As it is required that this document be reviewed annually, make sure the review date is included on this document.

8. **Payment Card Manager Compliance Certification Form**
   The Payment Card Manager Compliance Certification Form is a checklist verifying that the Payment Card Manager has completed all the required annual compliance documents, as well as the annual Self-Assessment Questionnaire (SAQ), and that these documents have been uploaded to the CampusGuard Document Locker. It is required that this document be renewed annually.

For information on completing the PCI DSS Self-Assessment Questionnaire (SAQ), or for samples and templates of the compliance documents shown above, visit the University of Minnesota Payment Card Program website.