

OUHSC Payment Card Security Standard

Purpose:

This standard is developed as required by the University Payment Card Security Policy. The purpose of this Payment Card Security Standard is to define roles and responsibilities for meeting the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and for the protection of the University information system resources that collect, store, process, and transmit cardholder data, or that could otherwise impact the security of cardholder data.

Standard:

Protecting the payment card information of our customers and maintaining compliance with the PCI DSS is a shared responsibility and requires each employee to understand and perform their part in the overall security of payment card data.

Roles and Responsibilities:

Office of the Bursar

The Office of the Bursar manages merchant services (credit card acceptance) for the University and is the point of approval and revocation of merchant accounts and the supporting hardware, software, and/or services. The Office of the Bursar will:

Manage the provisioning of Merchant ID's and merchant account and/or equipment requests related to payment card processing.

Validate and/or approve the hardware, software, services, and payment gateways that will be used for storing, transmitting, and/or processing cardholder data for the University.

Accept and evaluate, in coordination with the PCI Compliance Officer, all requests to store cardholder data to verify the business need and to ensure the merchant meets all the PCI DSS requirements for cardholder data storage.

Maintain a list of all merchant accounts that includes, at a minimum, the merchant ID, the payment card hardware/software associated with it, the ORG and department, and a primary and secondary point of contact.

Provide new merchant training that, at a minimum, will address the roles and responsibilities of the merchant staff under PCI DSS for the technology(s) to be used.

Maintain a list of all staff as identified by the merchant that are required to have the PCI training.

Track the total number of transactions occurring through the use of e-commerce solutions at least monthly.

Business Units

Business Units are ultimately responsible for maintaining compliance with current PCI DSS requirements within their environment and making sure all individuals are performing their roles as required and/or defined.

Each Business Unit must know and maintain a list of its merchant accounts and the supporting technology(s) approved for use by the Bursar and the PCI Compliance Officer.

Each Business Unit must know and document all individuals authorized to handle cardholder data in any format within the Business Unit and must ensure the completion of the appropriate training provided by the Office of the Bursar and the current Learning Management System (LMS), in accordance with the PCI DSS requirements. This training must be completed upon hire or prior to assignment of card handler duties and then annually thereafter.

If the Business Unit has approval from the Bursar to store cardholder data, the Business Unit must have policy(ies) and procedure(s) in place to meet the PCI DSS requirements associated with the storage of cardholder data as directed by the Office of the Bursar and the PCI Compliance Officer.

The Business Unit must have processes in place to distribute to their employees the policy(ies) and procedure(s) that address PCI compliance (samples available upon request) and must regularly assess overall compliance with them under the direction of the PCI Compliance Officer.

If the Business Unit cannot meet compliance requirements as defined by the PCI DSS, the Business Unit will work with Information Security Service for remediation and/or compensating controls to provide the intended protections of the PCI DSS.

If PCI DSS requirement(s) are to be met by a service provider or third-party external to the University on behalf of the Business Unit, the Business Unit must require that the PCI DSS requirement(s) to be met by the service provider or third-party are identified and documented, and have an agreement in place with service provider or third party that assures compliance with the designated PCI DSS requirement(s).

Credit Card Handlers

Credit Card Handlers are individuals who perform cashier, accounting, or other duties that interact directly with payment\credit card data.

Credit Card Handlers must complete the cardholder data training made available to them by the Bursars Office and/or the current LMS prior to handling any cardholder data and then annually thereafter.

Credit Card Handlers must review all Business Unit policy, standards, and supporting processes and procedures related to the handling of payment card data at least annually to stay abreast of what is required and expected of them by their Business Unit and the University.

Credit Card Handlers must adhere to all policy, standards, processes, and procedures of the Business Unit and University related to the protection and handling of cardholder data.

As provided in the training, Credit Card Handlers must regularly inspect the hardware utilized in performing or administering a payment card transaction for tampering as compared to the original Point of Interaction (POI) Characteristics document retained by the Business Unit for the device. This would include, but is not limited to terminals, card readers, PIN pads, desktops, or any combination of these technologies.

Credit Card Handlers must not disclose or acquire any information concerning a cardholder's account except as necessary to perform their job duties.

Procurement Staff

Procurement Staff are individuals who perform a role in acquiring or purchasing any software, hardware (products), or service(s) that store, process, transmit, or could impact the security of cardholder data.

To maintain overall compliance, Procurement Staff must manage the acquisition of these

products and services, assuring due diligence has been performed prior to purchase and/or engagement, which includes, at a minimum:

- Ensuring these products and/or services have been evaluated by Information Security Services prior to purchase.
- Ensuring these products and/or services have been verified and approved for compliance and supportability by the Bursar with the current merchant services provided.
- Ensuring that a written agreement is in place with any service providers or third parties who store, process, transmit, or otherwise impact the security of cardholder data; the agreement must define the PCI DSS requirements the service providers or third parties are responsible for and must require that PCI DSS compliance will be maintained and cardholder data will be protected.

IT Administrators and Developers

IT Administrators and Developers are System, Database, and Network Administrators and other staff who maintain or have privileged access to IT systems that may store, process, transmit, or impact the security of cardholder data; otherwise known as, Cardholder Data Environment (CDE).

All IT staff must know what systems in their environment are part of the University's CDE.

All IT staff who manage/maintain a system that is part of the University's CDE must ensure the system(s) is/are built, configured, managed, and/or maintained in accordance with current PCI DSS and applicable University IT Security Policy(ies).

All IT staff who manage/maintain payment software or hardware used to process payment card transactions must ensure all products are upgraded or replaced before the products' PCI SSC validation expires or when the product is identified as no longer PCI DSS compliant.

All IT staff must ensure any vendor or external/remote access to systems in the University's CDE is strictly monitored and performed in accordance with the current PCI DSS.

All IT staff will use encryption and some form of multi-factor authentication when accessing or managing any part of the CDE remotely (non-console access).

PCI Compliance Officer

The PCI Compliance Officer role, in coordination with the Office of the Bursar, Information Security Services, departments, and merchants, manages the PCI Compliance Program and the annual PCI risk assessment for the University.

The PCI Compliance Officer must obtain and maintain Payment Card Industry Internal Security Assessor credentials.

The PCI Compliance Officer will initiate the annual PCI risk assessment, confirm existing merchant IDs, distributing and collecting Self-Assessment Questionnaires (SAQs), and documenting and tracking any gaps in compliance.

The PCI Compliance Officer will assist merchant location and Business Units including credit card handlers, back office and procurement staff, and IT administrators and developers with understanding what the PCI DSS requirements mean and determining what requirements apply to them.

The PCI Compliance Officer will provide the Office of the Bursar any reports required for submission to the acquirer or card brands as requested.

Information Security Services

The Information Security Services (ISS) role is provided by the Information Security Services department and provides governance, risk management, and compliance support to the University for PCI DSS compliance.

ISS will define administrative and technical controls and procedures for securing cardholder data environments consistent with the PCI DSS for the University.

ISS will establish network vulnerability assessments, PEN testing, technology\control reviews, and risk assessments, as deemed necessary or required to support overall PCI compliance.

ISS will assist the Business Units\merchants with identifying compensating controls and remediation steps where requested.

Compliance and Enforcement: Failure to comply with this Standard or support the overall PCI compliance program requirements enforced by the Office of the Bursar or the PCI Compliance Officer could result in the suspension or loss of merchant account(s). This Standard is enforced by the Vice President of Administration and Finance or designee.

Scope: This Standard is applicable to Oklahoma University Health Sciences Center and its Tulsa campus counterparts. Any entity managing or using a software or hardware technology that stores, processes, transmits, or otherwise impacts the security of payment card data is responsible for complying with this Standard.

Regulatory Reference: Payment Card Industry (PCI) Data Security Standard
University of Oklahoma Policy

Definitions: See Information Technology Policy Definitions Document at <http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf>.

Policy Authority: This Standard is authorized and approved by the OUHSC Information Security Review Board (ISRB).

Table 1 Revision History

| Revision Date | Version | Revised By | Changes Made |
|---------------|---------|------------|--|
| 08/04/2011 | 1.9.6 | Campus IT | Baseline Version |
| 08/24/2011 | 1.9.8 | Campus IT | Updated to address new PCI DSS requirements |
| 02/20/2015 | 2.0 | Campus IT | Updated for better clarification of roles and responsibilities Updated to address new requirements in current PCI DSS |
| 06/16/2016 | 2.1 | Campus IT | Updated to address new requirements in current PCI DSS |
| 08/09/2016 | 2.2 | Campus IT | Verbiage changes for clarification |
| 10/03/2016 | 2.3 | Campus IT | Verbiage changes for clarification |
| 10/25/2016 | 2.4 | Campus IT | Verbiage changes for clarification |

Table 2 Approval History

| Version | Approval Date | Approved by: | Title: |
|---------|---------------|---|--------|
| 1.9.8 | 08/04/2011 | OU Health Sciences Center Information Security Review Board | |
| 2.4 | 11/08/2016 | OU Health Sciences Center Information Security Review Board | |

Table 3 Review History

| Version | Review Date | Reviewed by: | Title: |
|---------|-------------|-------------------------------|---|
| 1.9.6 | 08/24/2011 | Campus IT | Review for alignment to current PCI DSS |
| 1.9.8 | 10/15/2014 | Campus | Review for alignment to current PCI DSS |
| 2.0 | 02/20/2015 | Campus IT and Bursar | Review for alignment to current PCI DSS |
| 2.0 | 06/16/2016 | Campus IT and Bursars' Office | Review for alignment to current PCI DSS |