UNIVERSITY OF OKLAHOMA
Campus Payment Card Security Standard
Norman Campus

Subject: Campus Payment Card Security

Coverage: The University of Oklahoma—Norman Campus

Regulation: Payment Card Industry (“PCI”) Data Security Standards (“DSS”)
Version: 1.1.0

Effective: 01/01/2015

Revised: 08/27/2014

Purpose: The purpose of this Payment Card Security Standard is to provide University requirements for the protection of University information and information system resources that store, process or transmit cardholder data and for meeting the Payment Card Industry Data Security Standards (“PCI DSS”) and other compliance requirements for cardholder data.

Standards: The University establishes the following campus-level requirements and responsibilities supporting the University's governance of its Cardholder Data Environment:

Business Units
- Business units are responsible and accountable for all aspects of PCI compliance within their environment as well as all other aspects of the management and governance of their Cardholder Data Environment.
- Business units establishing or operating a system storing, transmitting, or processing credit card information must obtain written permission from both the CIO and General Counsel through the Office of the Bursar;
- Business units that store, process or transmit cardholder data must enter into and abide by all terms of the Office of the Bursar’s Merchant’s Contract;
- Business units will cooperate with the annual University compliance validation process coordinated through the Office of the Bursar and IT Office of Information Security;
- Business units storing, processing or transmitting cardholder data must comply with the most current PCI DSS requirements and procedures within the allotted grace period set forth by the Payment Card Industry Security Standards Council (“PCI SSC”);
- Business units authorized to store credit card information must have policies in place for data classification, retention, and disposition, addressing the secure and appropriate storage and disposal of the Cardholder Data and limiting the storage of Cardholder Data to only that which is required for business, legal and/or regulatory purposes;
- Business units that store, process or transmit Cardholder Data will follow the established University and Business Unit security standards and procedures for the Cardholder Data Environment;
- Business units must ensure that business unit policies, standards, and procedures are updated and maintained at minimum on an annual basis;
- Business units must apply the requirements of the PCI DSS to all employee and contract positions having responsibilities or activities that include the handling of Cardholder Data or other involvement in the
Cardholder Data Environment;

- Business units must document and maintain site-specific position descriptions for all workforce positions, new and existing, having responsibilities or activities that include the handling of Cardholder Data or other involvement in the Cardholder Data Environment, and must ensure that all responsibilities regarding the handling of Cardholder Data or involving the CDE are specified in the site-specific position descriptions;

- Business units must maintain online in the HRMS the site-specific position descriptions for employee positions with Cardholder Data related duties;

- Business units must establish procedures and arrangements for Cardholder Data training for all workforce positions and roles that handle Cardholder Data in any format;

- Business units must identify and keep record of all workforce members having responsibilities or activities that include the handling of Cardholder Data or other involvement in the Cardholder Data Environment, and must provide written notice to Human Resources of any employee having such responsibilities;

- Business units must obtain background checks for all current and prospective employees aged 18 and above who are to be retained in, hired, appointed, transferred, or promoted into a workforce position having responsibilities or activities that include the handling of Cardholder Data or other involvement in the Cardholder Data Environment, even if not explicitly required by the PCI DSS;

- Business units must initiate any and all background checks for workforce members through the Office of Human Resources;

- For workforce members whose responsibilities include handling Cardholder Data or other involvement in the Cardholder Data Environment, business units must ensure and keep record that, upon hire, appointment, transfer, or promotion and at least annually thereafter,
  - training is conducted for any such individual;
  - all workforce members certify that they have read, understand, and agree to all applicable university, campus, and departmental policy, standards, and procedures for payment card and Cardholder Data security;
  - all workforce members aged 18 and above certify that they have read, understand, and agree to all terms of an appropriate University non-disclosure/confidentiality agreement vetted and approved by the Office of Legal Counsel;

- Business units may not permit volunteers or minors to handle Cardholder Data or have other involvement in the Cardholder Data Environment, without official express permission granted by the OU Norman PCI Steering Committee and agreement to additional requirements specific to volunteers and minors.

- Business units must ensure that
  - access to system components, including physical access to Cardholder Data, is limited to only those individuals whose job duties require such access;
  - all primary account numbers (“PANs”) and expiration dates are masked on both the business unit and customer copies of the receipt, displaying no more than the last 4 digits of the PAN;
  - Cardholder Data is not transmitted using non-secure end-user messaging technologies such as email, instant messaging, or chat;
o all Internet connectivity on systems that process, store, or transmit Cardholder Data is restricted to that expressly approved for functionality related to processing credit cards and such systems are used for no other Internet activity.

- Business units must work with their respective IT support personnel and providers to ensure that all information technology related requirements of this standard and of the University Payment Card Security Policy have been met. Assurance of this compliance must be documented. The business unit is responsible for the following requirements, which it may carry out through its IT support function:
  o Implement and maintain administrative and technical controls and procedures for securing its Cardholder Data Environment consistent with the PCI DSS;
  o Assist and cooperate with vulnerability assessments, technology reviews, risk assessments, and compliance assessments deemed necessary or required by other governing bodies;
  o Fund, plan and perform any required remediation steps.

- Business units must obtain approval from the Office of the Bursar prior to making changes to existing environments, technologies and/or processes associated with Cardholder Data;

- Business units must obtain approval from the Office of the Bursar prior to entering into, or revising, any agreement for the provision of services by an External Service Provider;

- Business units utilizing any services from an External Service Provider must ensure that the current version of the University of Oklahoma PCI DSS Data Security Addendum, or other addendum as approved by the Office of the Bursar and the Office of Legal Counsel, has been duly executed.

- Business units utilizing any services from an External or Internal Service Provider must complete the University of Oklahoma PCI Responsibility Assignment for Management of Controls Matrix to document precisely which PCI DSS controls the service provider manages, which controls the merchant manages, and which controls are co-managed between the merchant and the service provider, and obtain documentation in writing by the service provider of its acceptance and acknowledgement of the specified division of responsibilities.

- In the event of a failure of safeguard efforts resulting in a breach or suspected breach of information, business unit will be responsible for:
  o providing, and all costs associated with providing, activities and actions for escalation, notification, and ex-post response, including but not limited to the following:
    ▪ escalation (preparations to report breach of protected information to appropriate entities within time requirements),
    ▪ notification (letters, outbound telephone calls, e-mail, public media, or general notice regarding the breach),
    ▪ ex-post response (arrangements facilitating breach victim communication with the University or University representative regarding questions and recommendations for minimizing potential harm, as well as redress actions including credit report monitoring or cost recovery for reissuance of new accounts or payment cards),
  o fines, judgments, and legal fees and expenses associated with the event,
corrective actions to remediate causes for the breach and actions to bring affected systems, environments, and entities into compliance,
reimbursement of costs incurred by other University departments and areas as a result of the incident, including costs of investigation, fines, judgment, and legal fees and expenses.

Office of the Bursar
- Assist business units with understanding the PCI DSS requirements;
- Maintain a list of all payment card hardware and software issued to business units for processing Cardholder Data;
- Manage approvals and provisioning of all merchant IDs;
- Provide Information Technology annually a list of all business unit merchant accounts and notify IT in the event of a change to the list;
- Provide Information Technology the number of payment card transactions and total dollar amounts on a per-merchant basis annually or as needed by a member of the IT Office of Information Security;
- Coordinate annual assessment services provided by a PCI Qualified Security Assessor (PCI QSA) for the purpose of providing an assessment report to the PCI Steering Committee for assurances needed for completing the Attestation of Compliance (AOC).
- Provide funding for PCI DSS regulatory compliance efforts, including
  - payment gateway services through TouchNet Information Systems, Inc.,
  - payment processing services through First Data Merchant Services and Unified Merchant Services,
  - university online portal for annual compliance validation tracking and reporting,
  - professional training of Bursar staff directly assigned to PCI compliance efforts, and
- quarterly network scanning services by an Approved Scanning Vendor (ASV) required as part of standard validation requirements. This funding does not extend to the payment applications, technologies, or remediation efforts of individual departments, or any cost associated with a breach or that is a result of a merchant data compromise (including on-site assessment services provided by a Qualified Security Assessor (QSA)).

Office of Human Resources
- Upon initiation by the business unit, conduct background checks as required by the PCI DSS;
- Work with the business unit to update and maintain position descriptions as necessary.

IT Support Function for Business Unit
- Work with the business unit to ensure the faithful implementation of all technical security requirements directed by the business unit;
- Provide documentation of technology implementation and evidences of technology compliance as requested by the business unit to support compliance validation processes.

Designated Local Campus IT Security and Compliance Function
- Assist business units with understanding the PCI DSS requirements;
- Provide vulnerability assessment, technology review, risk assessment, and compliance assessment services as deemed necessary by governing bodies;
- Assist the Office of the Bursar in the coordination of annual QSA assessment services;
- Assist the Office of the Bursar in providing the reports required for submission to the acquirer or card brands as requested.

**University of Oklahoma Computer Incident Response Team (CSIRT)**
- Provide incident response, investigation, and forensic services for security events impacting the Cardholder Data Environment.

**Scope/Applicability:**
This standard covers all components of the University of Oklahoma—Norman campus. This standard applies to all entities that collect, store, process, or transmit Cardholder Data, all entities that provide support for or oversight of Cardholder Data or System Components of the Cardholder Data Environment, and the additional entities specified herein with assigned roles and responsibilities. This standard applies to all System Components.

**Regulatory Reference:**
- PCI DSS 3.0 Requirements and Security Assessment Procedures,
- Oklahoma State Breach Notification Laws, Okla. Stat. §24-161 to 166, §74-3113.1],
- State of Oklahoma Information Security Policy, Procedures, Guidelines

**Definitions:**

**Consequences of Non-compliance:**
Failure to comply may result in the termination of a merchant’s ability to accept payment cards and/or fines assessed by the Office of the Bursar.

**Standard Authority:**
This standard is authorized and approved by the OU-Norman PCI Steering Committee.

**Authorization of Exceptions:**
Exceptions to this standard require a documented risk review and authorization by the OU-Norman PCI Steering Committee.

**Standard Compliance Audit:**
The University's Internal Auditing department is responsible for the auditing of compliance with this standard.

**Standard Enforcement:**
This standard is enforced by the Office of the Bursar.

**Renewal/Review:**
This standard is to be reviewed annually and updated as needed.