UNIVERSITY OF OKLAHOMA
Campus Payment Card Security Standard
Internal Service Providers

Subject:	Campus Payment Card Security Standard	**Coverage:**	Norman Campus
Regulation:	Payment Card Industry (“PCI”) Data Security Standards (“DSS”)	**Version:**	1.0.0
		Approved:	08/27/2014
Effective:	01/01/2015	**Reviewed:**	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:

Internal Service Provider

- The service provider is responsible and accountable for all aspects of PCI compliance related to hosting and all supporting services provided as well as all other aspects of the management and governance of the service provider’s provision of services affecting a customer’s Cardholder Data Environment.
- Internal service providers seeking to provide services storing, transmitting, or processing credit card information, or hosting or providing services affecting systems that do, must
  - obtain written permission from both the CIO and General Counsel through the Office of the Bursar; and
  - enter into and abide by all terms of the Office of the Bursar’s Internal Service Provider Contract.
- Internal Service Providers that provide services storing, transmitting, or processing credit card information, or hosting or providing services affecting systems that do, 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”);
  - follow the established University, Campus, and Service Provider security standards and procedures for the Cardholder Data Environment;
  - cooperate with the annual University compliance validation process coordinated through the Offices of the Bursar and the information security and compliance assessment;
  - ensure that service provider policies, standards, and procedures are updated and maintained at minimum on an annual basis;
  - implement and maintain administrative and technical controls and procedures for securing its Cardholder Data Environment consistent with the PCI DSS;
  - assist and cooperate with vulnerability assessments, technology reviews, risk assessments, and compliance assessments deemed necessary or required by other governing bodies; and
  - provide documentation of technology implementation and evidences of technology compliance as requested by the business unit to support compliance validation processes.

- Service providers 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;
- The service provider 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;
- Internal service providers must maintain online in the HRMS the site-specific position descriptions for employee positions with Cardholder Data related duties;
- Service providers must establish procedures and arrangements for Cardholder Data training for all workforce positions and roles that handle Cardholder Data in any format;
- Service providers 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;
- Service provider 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;
- The service provider 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, the service provider 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;
- Service providers 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 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.
- The internal service provider must
    - Obtain approval from the Office of the Bursar prior to making changes to existing environments, technologies and/or processes associated with Cardholder Data;
    - Assist the business units and the business unit IT support

personnel with remediation steps involving services provided by the provider;
    - Assist the Office of the Bursar in the coordination of annual QSA assessment services involving services provided by the provider
    - Assist the Office of the Bursar in providing the reports required for submission to the acquirer or card brands as requested steps involving services provided by the provider.
    - Provide precise and detailed statement of responsibilities via the University of Oklahoma *PCI Responsibility Assignment for Management of Controls Matrix,* to document which PCI DSS controls the service provider manages or co-manages and the service provider's acceptance and acknowledgement of the specified division of responsibilities.
    - Provide University merchants relevant requested information from the service provider's SAQ-D-SP as needed to support merchant compliance assurance and reporting.
    - Provide University merchants a signed copy of the *AOC SAQ D - Service Providers* completed by the service provider.

<u>Office of the Bursar</u>

- Assist the internal service provider with understanding the PCI DSS requirements;
- 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 service providers or individual departments, or any cost associated with a breach or that is a result of a data compromise (including on-site assessment services provided by a Qualified Security Assessor (QSA)).

<u>Office of Human Resources</u>

- Upon initiation by the service provider, conduct background checks as required by the PCI DSS;
- Work with the Internal Service Provider to update and maintain position descriptions as necessary.

<u>IT Support Function for Business Units</u>

- Work with the merchant's/business unit's service provider to ensure the faithful implementation of all technical security requirements agreed upon with the service provider;

<u>University of Oklahoma Computer Incident Response Team (CSIRT)</u>

- 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 internal service providers that collect, store, process, or transmit Cardholder Data or that provide services or support for University merchants or entities that do, 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, • 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘G–L–B Act’’), • Oklahoma State Breach Notification Laws, Okla. Stat. §24-161 to 166, §74-3113.1], • State of Oklahoma Information Security Policy, Procedures, Guidelines • Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681(c)(g).
Definitions:	See OU Payment Card Security Definitions document.
Consequences of Non-compliance:	Failure to comply may result in the termination of an internal service provider’s ability to provide services to OU merchants 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.