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

To establish organizational level security standards and procedures for the protection of cardholder data and compliance with the PCI DSS, all 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

Requirements:

- Business units that store, process or transmit cardholder data will follow the established security standards and procedures for cardholder data;
- Business units will cooperate with annual PCI risk assessments;
- Cardholder data storage must be limited to that which is required for business, legal and/or regulatory purposes, as outlined in the data retention policy;
- Disposal of media containing cardholder data must follow data disposal and/or media sanitization standards when no longer needed for business or legal reasons;
- All cardholder data must be classified as outlined in the "Data Classification Standard";
- All primary account numbers ("PANs") must be masked on both the business unit copy of the receipt as well as the customer receipt;
- All PANs electronically stored must be obfuscated (i.e., masked in accordance to the PCI DSS or encrypted);
- Other components of cardholder data must not be stored (please refer to the PCI DSS for more information);
- Access to system components, including physical access to cardholder data must be limited to only those individuals whose jobs require such access;
- Cardholder data must not be transmitted in an unsecure manner such as email, unsecured fax, or through campus email;
- Establish cardholder data training procedures for those that handle cardholder data in any format to be conducted upon hire and annually;
- Notify Information Technology prior to changes to existing
environments, technologies and/or processes associated with cardholder data.
Every business unit handling cardholder data must have a designated data owner. This person is typically at the executive management level or higher. In the event there is an individual(s) better suited for this responsibility, the data owner can designate who assumes this role. The data owner is responsible for the confidentiality and integrity of the cardholder data. *Every business unit is ultimately responsible for PCI compliance within their own environment.*

**Credit Card Handlers and Processors**

Requirements:
- Must have received training prior to handling cardholder data;
- All processes and procedures produced by the Business Unit Supervisor must be adhered to and strictly followed while handling cardholder data;
- University employees agree not to disclose or acquire any information concerning a cardholder’s account;
- E-commerce merchants using third-party software, including cash register systems processing through other service providers, are prohibited from storing cardholder data on the University network unless business requirements state otherwise;
- Other external merchants storing or transmitting cardholder data must be done in a secure manner as approved by Information Technology.

**Office of the Bursar**

Requirements:
- Provides approved equipment for processing cardholder data;
- Maintain a list of all payment card hardware issued to business units for processing cardholder data;
- Manages approvals and provisioning of merchant id’s for payment card processing;
- Provide Information Technology annually all business unit merchant accounts;
- Provide Information Technology annually the number of payment card transactions and total dollar amount.
- Provide funding for PCI DSS regulatory compliance efforts, including but not limited to, professional training of bursar and IT staff directly assigned to the PCI compliance efforts, applications related to the PCI reporting and monitoring efforts of the University compliance effort, and third party validation. This funding does not extend to the payment applications of individual departments.

**Human Resources**

Requirements:
- Inform workforce members upon hire and annually, training requirements for working in or having access to cardholder data environments;
- Track completed training requirements in HR system.

**Information Technology**

Requirements:
To implement and maintain administrative and technical controls and procedures for securing cardholder data environments consistent with the PCI DSS;

- Will establish network vulnerability assessments, technology reviews, risk assessments, and compliance audits as deemed necessary or required by other governing bodies;
- Will assist business units with understanding the PCI DSS requirements;
- Will assist the business units with remediation steps;
- Assist the Bursar’s Office by providing the reports required for submission to the acquirer or card brands as requested.

**Scope/Applicability:**
This standard is applicable to The University of Oklahoma and affects all staff that has responsibility for the collection, processing, storage and transmission of cardholder data including maintenance of system components of the cardholder data environment.

**Regulatory Reference:**

**Definitions:**
See IT Security Policy definitions document

**Responsible Department:**
The University of Oklahoma Office of the Bursar

**Standard Authority:**
This standard is authorized and approved by the OU Health Sciences Dean’s Council and Provost.

**Standard Enforcement:**
This standard is enforced by the University’s Office of Compliance.

**Standard Compliance Audit:**
The Internal Auditing department of the University of Oklahoma is responsible for the auditing and reporting of compliance with this policy.