Oklahoma State University Policy and Procedures

ELECTRONIC COMMERCE AT OKLAHOMA STATE UNIVERSITY	**3-0336 ADMINISTRATION & FINANCE April 2019**

Introduction and Guiding Principles

1.01 Oklahoma State University views electronic commerce as an additional outlet for contact with future alumni, faculty, staff, and the public. OSU encourages Colleges and auxiliary departments to utilize electronic commerce as a component of current business functions and interactions.

1.02 The use of credit cards or debit cards is a common and widely accepted practice of conducting payment transactions. Oklahoma State University allows departments within the university to establish themselves as credit card merchants to more fully participate in e-commerce at OSU.

1.03 The purpose of this policy is to establish guidelines and minimum requirements to be followed when accepting e-Commerce payments, specifically credit and debit card payments.

1.04 The Office of the Associate Vice President for Administration and Finance will have oversight responsibility for institutional provision that define electronic commerce, e-Commerce standards and procedures, and enforcement of payment card industry data security standards at Oklahoma State University.

Definitions

2.01 Electronic-Commerce

Business transactions over electronic means. This normally means the internet, but can include any electronic interaction – including automated phone banks, touch screen kiosks, or even ATMs. Transactions can include debit/credit cards (historically the primary method of e-Commerce payment), but also include any electronic transfer of funds via Automated Clearing House [ACH].

2.02 Payment Card Industry Data Security Standard [PCI DSS]

A consolidated standard from the major credit card issuers detailing merchant requirements when accepting credit/debit cards. The requirements include network, security (physical/logical), and monitoring components, among others.

2.03 Cardholder Data

Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number [PAN], name, expiry date, and card verification value 2 [CVV2] are included in this definition.

Scope

3.01 This policy applies to all University departments, employees, approved vendors, consultants, and other persons associated with the University wishing to conduct e-Commerce via any and all media and delivery mechanisms.

3.02 Individual units within the University may define 'conditions of use' for information resources under their control. These statements must be consistent with this overall policy, but may provide additional detail, guidelines, and/or restrictions. Such policies may not relax or subtract from this policy. Where such 'conditions of use' exist, enforcement mechanisms defined therein shall apply. These additional policies will be subject to review and approval by the Office of the Associate Vice President for Administration and Finance.

Policy

4.01 Any electronic commerce associated with Oklahoma State University must have a basis in University mission. Unrelated e-Commerce activity cannot utilize the university network or associated systems. A Payment Card Industry Security Standards Council (PCI SSC) validated Point to Point Encryption (P2PE) solution is required to utilize the University network for payment processing.

4.02 Any transaction, system, application, or process associated with e-Commerce (including credit/debit card transactions) will be performed in compliance with the PCI DSS, OSU standards and procedures for e-Commerce, and retain ongoing approval of the Office of the Associate Vice President for Administration and Finance.

4.03 E-Commerce activity will be performed within the centralized solution provided by Oklahoma State University administration unless a written exception is granted by the Office of the Associate Vice President for Administration and Finance.

4.04 The merchants grandfathered in as Self –Assessment Questionnaire [SAQ] C and D levels will hire external assessors to validate compliance with PCI DSS. The department responsible for the merchant will be required to pay for the assessor's report.

Compliance Failure Penalties

5.01 Failure to comply with this policy may have the following consequences:

A. Revocation of credit card acceptance for the affected unit.
B. Fines (up to $500,000.00) assessed to the responsible branch or department.
C. Legal action by injured parties.

D. Prosecution for criminal violations.

Special Notifications

6.01 Following OSU Policies and Procedures, Oklahoma laws and applicable federal laws, OSU strives to protect personal privacy and the confidentiality of information. Departments engaging in e-Commerce are responsible for safeguarding confidential information used in the processing of e-Commerce activity.

6.02 Cardholder information can never be transmitted across a network unsecured. Transport Layer Security 1.2 [TLS] at the very minimum is required to transmit cardholder data. Emailing unencrypted credit card numbers is never acceptable.

6.03 As a part of the OSU network, wireless connectivity is available for use in the same manner as a wired network jack. However, special considerations and additional security requirements from a PCI DSS standpoint are necessary when connecting to a wireless network for e-Commerce activities. For these reasons, Oklahoma State University has not authorized the use of any wireless network for e-Commerce activities.

6.04 The major regulatory body associated with credit card transactions is the PCI security Standards Council (www.pcisecuritystandards.org) and promulgates the rules and regulations OSU adheres to in the credit card environment.

Questions or Comments

7.01 Any questions or comments regarding this policy should be directed to:
Office of the Associate Vice President for Administration and Finance
207 Whitehurst
Stillwater, OK 74078
405-744-4188
PCI@okstate.edu

Approved:
December 2003

Revised:
October 2007
April 2019

Approved by E-Team:
January 2008
June 2012
January 2013
May 2019