University of Oregon

Policy Statement Development Form

Policy Title:
Electronic Commerce

Policy submitted by:

Name: Mark McCulloch
Phone: 541 346-6249
Email: mmccullo@uoregon.edu
Organization: Business Affairs
Date: July 2014

Preamble:
Electronic commerce as a natural extension of university business processes. All units are encouraged to utilize electronic commerce to improve service to students, faculty, staff, and the public, and to reduce the cost of providing these services.

It is important that entities processing credit card payments take measures to safeguard sensitive customer information and reduce the risk of data breach.

A data breach exposing cardholder data has far-reaching consequences for affected organizations, including:

1. Damage to reputation/brand,
2. Loss of customers,
3. Financial impacts (cost of response effort including; customer notification, call center activity, consulting, PR, lost productivity, litigation, and fines)

Reason for Policy:
This policy established rules for credit card and electronic payment processing activities at the university of oregon that safeguard customer card data, and ensure compliance with global security standard PCI DSS.

Who is Governed by this Policy:
(*Please mark all that apply*)
_X_ Faculty
___ Students
_X_ Staff
_X_ Other: Student Employees

Who Should Know this Policy:
Employees involved in processing customer debit/credit cards or electronic check payments.

Policy Statement:

1. The Director of Business Affairs is responsible for,
    - Ensuring university compliance with Payment Card Industry Data Security Standards (PCI DSS), and state laws regarding the proper handling of state funds,
    - The distribution of related policies and procedures.
    - Authorizing all debit/credit card activities at the University of Oregon.
2. University merchants authorized to process customer debit/credit cards will validate their PCI DSS compliance status each year to Business Affairs by preparing the appropriate Self Assessment Questionnaire (SAQ) and carry out any necessary remediation.
3. University merchants must obtain approval from Business Affairs before contracting with a third party service provider for debit/credit card processing products or services.
4. University merchants shall not store cardholder data in electronic form or transmit it in clear text, unencrypted.
5. Storage of paper records containing customer card data is strongly discouraged. Maximum retention is 3 years.
6. University merchants shall avoid processing customer card data on university computers and favor lower risk processing methods:
    - Fully hosted PCI compliant, third party customer online payment solutions,
    - Dedicated, PCI compliant, third party point of sale equipment.
7. Employees involved in credit card processing, IT professionals that support the UO card data environment, and purchasing and leasing agents who craft agreements with third parties who may process credit cards on campus or on behalf of the university, must participate in the Business Affairs PCI security awareness training annually.
8. The university will maintain risk assessment program that identifies assets, threats, and vulnerabilities related to university credit card processing policy, training and security practices. A formal risk assessment will be undertaken each year.
9. In the event of a data breach involving customer card data the university will execute its incident response plan, http://ba.uoregon.edu/staff/ecommerce#Incident_Response_Plan
10. Business Affairs will review and update this policy on an annual basis as security threats and protection methods evolve.

Procedures:

Procedures for implementing this policy are published on the Business Affairs website under Cashiering and Commerce,

http://ba.uoregon.edu/staff/ecommerce

Definitions:

Customer Card Data
At a minimum, cardholder data consists of the full PAN (Primary Account Number). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Electronic Commerce
For purposes of this policy, electronic commerce includes the sale of university property or services accomplished using an electronic medium such as debit/credit cards or electronic check payments.

PCI DSS
Payment Card Industry Data Security Standard. Credit card processing security standards established and maintained by the PCI Security Standards Council for merchants and processors. The PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to enhance payment account data security.

PA DSS
Payment Application Data Security Standard. Security standards established by the PCI Security Standards Council specifically for payment applications such as point of sale systems that accept credit cards.

SAQ
Annual Self Assessment Questionnaire is one method for merchants to validate that they are in compliance with PCI DSS. There are five different self assessment questionnaires (SAQs) (A,B,C, C-VT and D) each is designed for different credit card processing methods and risk levels.

Forms/Instructions/Regulations:
eCommerce Activity Request Form
Third Party Payment Processor Request Form
Business Affairs eCommerce Services and Instructions

Cross Reference to Related Policies:
PCI DSS

Responsible University Office:
University Office: Business Affairs
Office Website URL: http://ba.uoregon.edu/

Policy Owner: Director of Business Affairs
Email: kbwolf@uoregon.edu
Phone: 541 346-3165

Related Documents:

Frequently Asked Questions:

Revision/Development History:
Originally published by Business Affairs 22 March 2001 and revised over time.

Organizational Category:
*(Please mark **only** one)*

____ Administration and Governance
____ Academic and Curricular
____ Human Resources
____ Facilities
____ Students
_X__ Finance and Business Affairs
____ University Relations
____ Health and Safety
____ Research
____ Information Technology
____ General

POLICY CONSULTATION AND REVIEW

*Consultation and review by the following individuals or groups (**optional**):*

_____
Print Name Date

_____
Print Name Date

_____
Print Name Date

_____
Print Name Date

……

REVIEWED AND APPROVED BY:

Executive Leadership Team _____

Signature Date

ISSUED BY:

Office of the Senior Vice President and Provost _____

Date

POLICY EFFECTIVE DATE: _____

Date

ASSIGNED POLICY NUMBER: _____