Policy Title:
Electronic Commerce

Policy submitted by:
Name: Mark McCulloch
Phone: 541 346-6249
Email: mmccullo@uoregon.edu
Organization: Business Affairs
Date: Feb 2012

Preamble:
The university views electronic commerce as a natural extension of its business processes. We encourage colleges and auxiliary departments 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 university entities processing credit card or electronic check payments take measures to safeguard sensitive customer information. A security breach and compromise of cardholder data has far-reaching consequences for affected organizations, including:

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

Reason for Policy:
This policy provides guidelines for all credit card and electronic payment processing activities at the University of Oregon.

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,
   • University compliance with Payment Card Industry Data Security Standards (PCI DSS), and state laws regarding the proper handling of state funds, and
   • 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 must validate their compliance with PCI DSS each year by completing the appropriate Self Assessment Questionnaire (SAQ) and carrying out any necessary remediation. Business Affairs coordinates the annual self assessment process and security awareness program and identifies threats and vulnerabilities for formal risk assessment by Internal Audit Division.
3. University merchants shall not store cardholder data in electronic form or transmit it in clear text, unencrypted. Storage of paper records containing customer card data is strongly discouraged.
4. 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.
5. University merchants must obtain approval from the Business Affairs before contracting with any third party service provider for debit/credit card processing products or services.

Procedures:
1. Units with a business need to process customer credit cards request authorization by completing the eCommerce Activity Request Form.
   
2. Business Affairs provides university merchants with a secure customer online payment solution at no cost. Funds are deposited automatically in Banner and the annual PCI DSS SAQ is completed by Business Affairs.
3. Units authorized to process customer credit cards must maintain the following standards:
   (a) If you have a business reason to create paper records containing full PANs, mark them ‘Confidential’, physically secure them, limit access to full time professional staff with a business purpose, inventory them every six months, and confidentially recycle within 36 months.
   (b) Ensure access to electronic records is authorized in writing by the employee’s manager.
   (c) Do not send or receive complete credit card numbers using email, campus mail or unsecure wireless networks.
   (d) Comply with appropriate accounting standards established by the Vice President for Finance and Administration.
   (e) Uniquely serialize and fully journalize all transactions to provide a conclusive audit trail.
   (f) Routinely reconcile all goods and services provided and received with the accounting records.
   (g) Designate a unit information security officer or single point of contact.
   (h) Train all employees with access to protect cardholder data upon hire and annually, and ask them to review this eCommerce policy annually and when business processes change. Use letters, posters, memos, meetings and promotions to increase employee awareness.
(i) Develop daily operating security procedures (desk manuals) for workers with access to cardholder data that are consistent with PCI DSS. Require employees to sign verifying that they understand the security procedures or include them in a signed position description.

(j) Obtain approval from the Oregon State Treasurer before contracting with third party service providers for debit/credit card processing services or applications. Vendors must complete the OST Third Party Payment Processor Pre-Qualification.

(k) Each year Business Affairs coordinates the annual PCI DSS SAQ process. Campus merchants will complete the appropriate SAQ and carry out any remediation necessary for full PCI DSS compliance.

(l) Do not store cardholder data on university computers or on portable devices and media.

(m) If practical, disconnect modems used for card processing at point of sale when they are not needed or automatically after a period of inactivity.

(n) Maintain a list of all payment terminals (make, model, location, serial number) and train staff to inspect them periodically for tampering or substitution.

(o) If customer cardholder data is shared with service providers, include language in the contract or agreement that obligates the service provider to maintain PCI compliant status and assume responsibility for the security of cardholder data in their possession.

4. Business Affairs will review and update this policy on an annual basis as security threats and protection methods evolve.

5. Incident Response Plan

Customer data security can be compromised in a variety of ways, such as:

- Active malware infection where the malware allows unauthorized remote access into the system or allows the unauthorized retrieval of data from the machine. This does not include the quarantine of incoming malware that does not actually execute on the system in question.
- Unintended disclosure on a public website or through physical or electronic mail.
- Payment card fraud involving skimming devices at point of sale terminals
- Lost or stolen paper documents or computing equipment (laptop, PC, or backup media) containing unencrypted personal information.

In the event that paper or electronic records containing personal data are potentially exposed to unauthorized persons, units shall take the following steps:

**A. The Affected Unit** shall;

- Immediately contain and limit the exposure of data.
- Alert the appropriate Records Custodian (Registrar, AVP HR, Dir Business
Affairs, Dir Health Center, or Dir Human Research Protection Program) and General Counsel.

- Conduct an immediate and thorough investigation of the suspected exposure or theft of personal information.
- Not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
- Not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the cable).
- Work with Network Services to preserve logs and examine electronic evidence and if using a wireless network, change SSID on the AP and other machines that may be using this connection.
- Maintain a log all actions taken.
- Provide the records custodian and General Counsel with an incident report containing; all information at risk and the source and timeframe of the compromise.
- Notify affected customers if directed by General Counsel
- Remediate as directed by the Records Custodian

B. Network Services, has intrusion detection and monitoring systems, and trained personnel available 24/7 to respond to network alerts involving the potential exposure of electronic records. Network Services will immediately work with technical staff in the affected unit to evaluate and provide evidence that would indicate that personal data was reasonably believed to have been accessed by an unauthorized person to the incident response team.

C. The UO Incident Response Team (Dean/Dir of the affected unit, Records Custodian, CIO, Vice President Finance and Administration, Office of the General Counsel, Risk Management, Media Relations, and Public Safety) will consider the evidence provided by the affected unit, the Records Custodian and Network Services, and decide whether or not the following actions are warranted;

- Notify Internal Audit Division
- Engage local law enforcement, FBI, CIA
- Notify affected customers
- Notify other third parties for breaches involving; credit cards, educational records, health records, research subject data, donor information, or other records.
- Prepare a press statement or release
- Prepare a post mortem report with action log and remediation plan for affected unit.

The Incident Response Team will evaluate and evolve the incident response plan based on lessons learned in responding to potential breaches.

D. Records Custodian (Registrar, AVP HR, Dir Business Affairs, Dir Health Center, or Dir Human Research Protection Program) shall;
- Notify IAD and other third parties as directed,
- Work with Media Relations and General Counsel on customer notification text and scripts as directed, and
- Prepare a post mortem report with action log and remediation plan for affected unit.

**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
- OST Third Party Payment Processor Pre-Qualification
- Business Affairs eCommerce Services and Instructions
Cross Reference to Related Policies:
PCI DSS
OST Cash Management Policy 02 18 14.PO

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:
Incident Report

Frequently Asked Questions:
[Insert any FAQs]

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):