

IT02 UO eCommerce Policy

Effective 22 March 2001

Last Revised 24 Mar 2008

Who Should Read This Policy

Administrators for UO entities that are processing credit card, online credit card, or electronic check payments.

Background & Purpose

The Business Affairs Office views electronic commerce as a natural extension of the business processes already conducted by the University. 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. For purposes of this policy, electronic commerce includes all business transactions accomplished using an electronic medium.

It is important that UO entities processing credit card or electronic check payments take measures to safeguard sensitive customer information including credit card numbers. Failure to comply with Payment Card Industry (PCI) rules may result in financial loss, fines, suspension of credit card processing privileges, and/or damage to the reputation of the university.

This policy provides guidelines for all credit card and ePayment processing activities at the University of Oregon.

Policy

1. The Director of Business Affairs is responsible for university debit/credit card security, the distribution of security policies and procedures, monitoring of system access and alerts, and incident response.
2. The Director of Business Affairs shall approve all eCommerce activities at the University of Oregon, including: card present or point of sale transactions, transactions conducted over the phone, by fax, and/or on the internet.

eCommerce Activity Request Form

<http://baowww.uoregon.edu/forms/cca.pdf>

3. University departments with approved credit card processing activities must maintain the following standards:

a) Protect Customer Information

- Do not store, process, or transmit credit card data on the university network. Instead, use Office of the State Treasurer (OST) approved, secure, and fully hosted third party payment processing services.

- Do not create an electronic file containing full credit card numbers (database, spreadsheet, word processor, image, etc.)
- Avoid the retention of paper records containing complete credit card numbers. If, for business reasons, you must store full card numbers then do so for no longer than 36 months before securely disposing of them (confidential recycle, cross-cut shred, pulp, or incinerate). Mark these records as 'Confidential'.
- Records containing partial card numbers should be retained for no longer than seven years.
- Strictly limit access to paper records containing credit card and bank account numbers based on job function. Where practical, limit access to full time professional staff.
- Access to electronic records must be authorized in writing by the employee's manager.
- Hypercom terminals must be programmed to mask card numbers on both merchant and customer copies of receipts.
- Physically secure paper records containing full credit card numbers in locked cabinets or offices with adequate key control.
- Inventory paper records containing full or partial credit card numbers every six months to identify loss or theft of items.
- Do not send or receive complete credit card numbers using email or campus mail.

b) Properly Account

- Adhere to appropriate accounting standards as established by the Vice President for Finance and Administration.
- Uniquely serialize and fully journalize all transactions to provide a conclusive audit trail.
- Routinely reconcile all goods and services provided and received with the accounting records.

c) Employee Training

- Designate a unit information security officer or single point of contact.
- Train all employees involved in processing card transactions to protect card data and ask them to review this policy annually and when business processes change.

d) Annual Risk Assessment

- All university units processing credit cards will participate in an annual PCI risk assessment.

e) Third Party Vendors

- The Business Affairs Office (BAO) will assist university departments in processing credit card and echeck payments online using fully hosted payment processing services that are approved by the Office of the State Treasurer (OST). These services are Payment Card Industry (PCI) compliant, NACHA compliant, and cost effective.

- In accordance with OST Cash Management Policy 02 18 14.PO, all third party vendors must be approved in advance by OST. To obtain approval vendors must complete the OST 3rd Party Vendor Prequalification Form, <http://baowww.uoregon.edu/ecommerce/OSTVendorApp.doc>
- Oregon law requires that state funds be deposited directly into a recognized Oregon depository within 24 hours. For this reason the use of **PayPal** or similar services that do not deposit proceeds directly into an OST merchant account are prohibited.

4. Incident Response Plan

In the event of a breach in card data security take the following steps:

A. The unit shall immediately contain and limit the exposure of cardholder data. Alert Business Affairs, and conduct a thorough investigation of the suspected loss or theft of account information.

- Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
- Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the cable).
- Preserve logs and electronic evidence.
- Log all actions taken.
- If using a wireless network, change SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised).
- Be on high alert and monitor all systems with cardholder data.
- Provide Business Affairs with a report containing; account information at risk and the source and timeframe of the compromise.

B. Business Affairs will alert all necessary parties immediately.

Note: If an incident occurs during normal business hours (8:00AM to 5:00PM), notify the Office of the State Treasurer (OST) by using the number listed below. OST will then notify U.S. Bank, and coordinate all communication. If an incident occurs outside of normal business hours, contact U.S. Bank directly by using the phone number listed below.

- **Internal Information Security group and Incident Response Team.** University of Oregon; CIO, VP Finance and Administration, Office of the General Counsel, Dir Human Resources, and Media Relations
- **Office of the State Treasurer (OST); (503) 378-4000.** Notify the receptionist that you have experienced a merchant card breach, and ask

to speak with the Merchant Bank Liaison on the Banking Team or a member of the Relationship Management Services team.

- **U.S. Bank; 1(800) 725-1243.** Identify that you are a “**National Account**” under State of Oregon, and provide them with your **Merchant ID (MID) #**. Notify the U.S. Bank customer service representative that you have experienced a merchant card breach, and ask that the incident be reported to the Risk Department.

C. Business Affairs will complete the attached Incident Report as soon as possible.

Note: This must be completed within three business days, and provided to the Office of the State Treasurer. OST will forward it to U.S. Bank/NOVA. Visa and U.S. Bank/NOVA will determine and notify the agency and OST if an independent forensic investigation, compliance questionnaire, and vulnerability scan are required.

Authority

The UO Vice President for Finance and Administration has authority for administering this policy and has delegated its implementation to the Director of Business Affairs.

References

- BAO Payment Processing Services
<http://baowww.uohosting/>
- Credit Card and ePayment Activity Request Form
<http://baowww.uoregon.edu/forms/cca.pdf>
- UO Credit Card Handling Procedures
<http://baowww.uoregon.edu/cashiers/CreditCardHandling.htm>
- Oregon State Treasury Cash Management Policy
<http://baowww.uoregon.edu/ecommerce/OSTCashMgtPolicy.doc>
- Oregon State Treasury 3rd Party Vendor Prequalification Form
<http://baowww.uoregon.edu/ecommerce/ostvendorapp.doc>
- OUS Policy Guideline for Electronic Commerce
<http://www.ous.edu/cont-div/fpm/elec.40.005.php>
- Payment Card Industry Data Security Standards (PCI DSS)
<https://www.pcisecuritystandards.org/index.htm>

Contact

Business Affairs 346-6249

Incident Report

Merchant Name:

Merchant ID #:

Date of Incident:

Bank Use Only:

MCC:

BIN/ICA:

What is the transaction date range associated with the compromise accounts?

What credit card data was compromised?

Was your system storing track 1 or track 2 data?

Was your system storing CVV/CVC 2 data?

How many credit cards were involved?

Was law enforcement notified, and if so, which department/agency?

What steps have been taken to remediate the risk/vulnerabilities?

How did the compromise occur?

What are the compromised systems?

Has all possible evidence been preserved?

What software and what version are you running?

Are you PCI Compliant?

Actions Taken:

Actions Pending:

Contact Information: