UNIVERSITY OF OREGON

POLICY IV.4.1
Payment Card Acceptance

Reason for Policy

This policy establishes roles, responsibilities and rules for debit/credit card processing activities at the University of Oregon and is designed to safeguard Customer Card Data, reduce the risk of card data breach, and facilitate compliance with global payment card industry data security standards.

Entities Affected by this Policy

Faculty, Staff and Student Employees

Web Site Address for this Policy

https://policies.uoregon.edu/payment-card-acceptance

Responsible Office

For questions about this policy, please contact the Business Affairs Office at 541-346-3165.

Enactment & Revision History

Approved by Dr. Scott Coltrane, Interim President on June 30, 2015

Policy

PREAMBLE

Consumer preferences for debit and credit card payment has steadily increased during the past decade, while cash and check use in particular has declined. The convenience of online payment is a key driver. Cash is still common for small dollar transactions, especially in food service and transportation. Cash and checks are labor intensive and costly means of payment collection.

Some university departments sell goods and services, (particularly events), to students, faculty, staff, and the public. These departments are encouraged to offer debit/credit card payment options both in person and online to improve service and reduce collection costs.

University departments accepting debit/credit card payments must take measures to safeguard Customer Card Data, reduce the risk of data breach, and comply with the Payment Card Industry (PCI) rules.

A data breach exposing cardholder data can have significant consequences including:

1. Damage to university reputation or brand,
2. Loss of customers (students, donors),
3. Financial costs (fines, card re-issue fees, customer notification, credit monitoring, forensic investigation, public relations, and litigation).

DEFINITIONS

University Merchant

Any university department that accepts customer debit/credit card payments.

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.

Ecommerce

Card processing method where the customer enters their card data into a web page or application using their personal device.

PCI DSS

The Payment Card Industry Security Standards Council (PCI SSC), founded by major brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. created global security standards that apply to all merchants and service providers worldwide to enhance payment account data security.

The PCI security standards include the Payment Card Industry Data Security Standard (PCI DSS) for merchants and service providers, the Payment Application Data Security Standard (PA-DSS) for software vendors, and the PIN Transaction Security (PTS) for device vendors and manufacturers.

SAQ

Self-Assessment Questionnaire (SAQ) is one method for merchants to validate their compliance with PCI DSS. There are eight distinct SAQs (A, A-EP, B, B-IP, C, C-VT, D, and P2PE-HW) each designed for different credit card processing methods and environments.

Data Security Incident Response Plan

The plan that is executed by the Data Security Incident Response Team in the event of a potential data breach.

POLICY STATEMENT

1. The AVP Business Affairs/Controller is responsible for,
   a) Ensuring university compliance with PCI rules, merchant banking contract terms and conditions, and state law regarding proper handling of public funds.
   b) The distribution of related policies and procedures.
   c) Authorizing all debit/credit card activities at the University of Oregon.

2. University Merchants authorized to accept debit/credit card payments will validate their compliance status with PCI DSS at the end of each calendar year. Compliance gaps must also be remediated by University Merchants in a planned and continuous effort throughout the year. Failure to come into compliance with PCI DSS may result in the loss of card acceptance privileges.

3. University Merchants will limit access to Customer Card Data to employees with a legitimate business reason, and will maintain standard operating procedures for its processing, protection and disposal.

4. University Merchants will obtain approval from Business Affairs before contracting with a third party for card processing services or solutions.

5. University employees shall not store Customer Card Data in electronic form on the university network, or send or receive unencrypted cardholder data (for example by email or text message).

6. University employees will avoid creating paper records that contain Customer Card Data. Paper records containing Customer Card Data must be confidentially recycled immediately after processing or when the business reason for retention ends. Maximum retention is 1 year.

7. Whenever practical, University Merchants shall adopt low risk processing methods such as:
   - Ecommerce, fully outsourced to service providers validated by the PCI Security Standards Council.
   - Purpose built payment card terminal, certified by the PCI Security Standards Council.

   University employees will not enter Customer Card Data on a university computer without a compelling business reason. University computers used to process or transmit Customer Card Data must be; hardened, dedicated to this purpose (never used for email, social networking or web browsing), firewalled, segmented from other devices, and scanned for vulnerabilities by an Approved Scan Vendor (ASV).

8. The following personnel will participate in formal security awareness training annually;
   - Employees involved in accepting customer credit card payments.
   - IT professionals supporting university systems that host pay buttons or that process or transmit Customer Card Data.

- Purchasing and leasing agents who craft agreements with third parties who process credit cards on campus or on behalf of the university.

9. In the event of a data breach involving Customer Card Data the university will execute its Data Security Incident Response Plan.

RELATED RESOURCES

Procedures for implementing this policy are published on the Business Affairs website

Forms/Instructions/Regulations:

1. Business Affairs Payment Card Services and Instructions
2. Payment Card Acceptance Request Form
3. PCI Security Standards Council