Policy Title:	PCI Compliance Policy

Governing Body:	Finance and Administration	Policy Number:	FAD .090
Policy Contact:	Bursar	Date Approved:	11/20/25
Custodial Office:	Business Services		
Approved By:	President Bailey		
Related Policy:	FAD.040 Information Security Policy Cash Handling Manual		

A. Description

Oregon regulations require that all processors of electronic commerce comply with the Payment Card Industry (PCI) Data Security Standards. The Office of the Oregon State Treasurer (OST) issued two Cash Management Policies to address these issues. The policies are 02.18.13.PO Data Security and 02.18.14.PO 3rd Party Vendor Requirements.

For purpose of this policy, electronic commerce includes all payment transactions using an electronic medium to process payments made by credit and debit cards.

It is important that Southern Oregon University (SOU) entities processing credit card or electronic payments take measures to safeguard sensitive customer information including credit card numbers. Failure to comply with 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 applies to **all Southern Oregon University (SOU) personnel and affiliated entities** that **store, process, or transmit** cardholder data or that manage the systems and networks in which cardholder data is stored, processed, or transmitted.

This includes, but is not limited to:

- **All SOU Employees** (full-time, part-time, temporary, student workers, and volunteers).
- **SOU Contractors and Consultants** who have access to SOU systems or cardholder data environments.
- **All Organizations, Clubs, or Entities** whose credit card payment processes or financial accounts are managed by or tied to SOU.

Third-Party Service Providers that store, process, or transmit cardholder data on SOU's behalf **must be PCI compliant and are required to provide SOU with documentation of their ongoing compliance**. Compliance with PCI is a **mandatory contractual requirement** for all third parties engaged for payment processing services.

SOU seeks to ensure that the policies and procedures related to accounts receivable and collections are documented, communicated, clearly understood, and consistently applied.

B. Definition(s)

PCI-DSS – Payment Card Industry Data Security Standards. This is the regulatory framework that determines our PCI compliance.
PCI Team – SOU personnel who oversee the university's PCI compliance efforts. The PCI Team should include personnel from Business Services, the Information Security Team, and the department of Information Technology. Current members are documented in the PCI Procedures document.
QSA – Quality Security Advisor. An expert certified in PCI compliance. SOU's QSA will be documented in the PCI Procedures document.
SAQ – Self-Assessment Questionnaire, used to attest compliance with the PCI-DSS.
OST – Office of the State Treasurer.
POI – Point of Interaction devices (e.g., card readers).
Merchant – Any campus group or department that takes credit card payments or donations made via credit card.
Merchant Lead – The SOU employee in charge of a group who processes credit card payments. The Merchant Lead could be a Department leader or a designee who manages the payment process for the Merchant.
CDE – Cardholder Data Environment. The interconnected network of systems that process, store, or transmit credit card information.
Payment Processor – Any third party that accepts or processes credit card payments for clients. E.g., PayPal, Square, Transact/CashNet.

C. Policy Statement

All Merchants and Payment Processors in operation on behalf of Southern Oregon University must be registered with the PCI Team and authorized to operate by the PCI Team prior to processing credit card transactions on behalf of SOU. It is a serious violation of policy for any campus group to begin accepting payments on behalf of a university program outside of approved channels or without prior approval from the Business Services office.

The PCI Team will retain a QSA and perform annual SAQs for each Merchant accepting credit card transactions. Merchants will cooperate fully with the PCI Team in the compliance process as an ongoing requirement of processing payments on behalf of SOU.

The PCI Team will inventory all system components that are in-scope for PCI-DSS, including a list of hardware and software and a description of their function. Merchants are responsible for assisting the PCI Team with maintaining an accurate inventory. The PCI Team will review and update the inventory at least annually. Details of the inventory can be found in the PCI procedures document.

Merchants are responsible for maintaining the security of the Cardholder Data Environment (CDE) where the CDE intersects with their personnel and operations. (For example, Merchants are responsible for protecting the credit card readers in their possession and protecting their passwords.) Merchants are responsible for notifying the PCI Team of any changes in their area that might impact the CDE. All changes to the CDE must be approved by the PCI Team.

Merchants are responsible for ensuring that their staff understand and comply with the security measures as outlined in this policy and the companion PCI procedures. Merchants conducting cashiering activities are responsible for adhering to the university's Cash Handling Manual and ensuring that their personnel follow procedures for processing credit and debit card transactions.

Department managers who oversee Merchants in their administrative units are responsible for identifying Merchant Leads to the PCI Team. Merchant Leads shall be primarily responsible for all Merchant duties outlined in this policy, with department managers serving as backups in the event of a vacancy or absence in the Merchant Lead position.

All personnel involved in payment processing for a Merchant will review this policy and the companion PCI procedures and sign an annual statement of understanding before processing payments. These records are maintained by Business Services and subject to internal audit. Merchant Leads or department managers must notify the PCI Team of all changes to personnel who handle payments for the Merchant, including offboarding of personnel who no longer need access to the CDE. Only authorized personnel are permitted to conduct credit card transactions on behalf of the university.

Merchants are responsible for promptly reporting lapses in security, breaches, and any other security incidents that involve the CDE or cardholder data according to the procedures in the PCI procedures document. Merchants will cooperate with all incident response efforts in the event of a security incident. The PCI Team will develop and maintain incident response plans specific to PCI security incidents and will conduct PCI incident response in coordination with the Information Security Team (who should be represented on the PCI Team).

Failure to comply with the PCI-DSS standard, this policy, or the companion PCI procedures may result in a Merchant losing their payment card privileges. Personnel responsible for major lapses in compliance, or misconduct, may face disciplinary actions.

This policy may be revised at any time without notice. All revisions supersede prior policy and are effective immediately upon approval.

D. Relevant Authority

E. Other Information

OST PCI security policies at https://www.oregon.gov/treasury/public-financial-services/banking-with-treasury/pages/cash-management-policies.aspx:

02.18.13 Data Security

FIN 214 Third Party Vendor Requirements

Third Party Vendor Application

PCI Procedures (reference here)

The Policy Contact, defined above, will write and maintain the procedures related to this policy and these procedures will be made available within the Custodial Office.