PCI Compliance Procedures 200.080cd

Office: **Business Services**
Procedure Contact: **Bursar**
Related Policy or Policies: **n/a**

Revision History

Revision Number:	Change:	Date:
001	Update content and format	12-04-2017

A. Purpose

SOU adheres to Oregon State regulations that 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 purposes of this procedure, electronic commerce includes all payment transactions using an electronic medium to process payments made by credit and debit cards whether in a card present transaction or on-line.

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 procedure applies to permanent and temporary employees of SOU, including student workers and contractors.

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

B. Definitions

- PCI-DSS - Payment Card Industry Data Security Standards
- QSA – Quality Security Advisor (Coalfire)
- Coalfire – Independent cyber risk management advisor
- SAQ – Self-Assessment Questionnaire (self-review to attest compliance to the PCI-DSS)
- OST – Office of the State Treasurer

C. Procedures

SOU will retain a QSA and perform an annual SAQ. Departments will cooperate fully with Business Services and Information Technology staff regarding participation in the annual compliance review, inventories, follow up to security questions, and remediation of gaps and risks uncovered during the review or at any time throughout the year.

PCI Compliance Procedures 200.080cd

Departments accepting payment for services and products are responsible for ensuring that their staff understand the security measures as outlined in this policy. Departments conducting cashiering activities are responsible for adhering to the university's Cash Handling Manual and that personnel maintain the following standards for processing credit and debit card transactions.

All personnel involved in payment processing will review the compliance policy and sign an annual statement of understanding. See Appendix for User Data Security Verification Statement. These records are maintained by Business Services and subject to internal audit. Newly hired or re-assigned personnel who process payments will be required to read the policy and sign the statement. Department heads are expected to notify Business Services of changes to personnel including terminations.

Electronic data processing:
Do not store, process or transmit credit card data on the university network. Instead use OST approved, secure and fully hosted third party payment processing services. The use of USB-enabled devices and card readers is prohibited, e.g., smart phones, ipads, tablets, Square card reader, etc. Only SOU provided laptops and PCs operating on the restricted and secure network are allowed. WiFi (wireless) is prohibited for sensitive data processing. If your department uses or begins using an approved hosted payment processing site, the PCs and laptops must the on restricted network.

Do not create an electronic file containing full bank account or credit card numbers (database, spreadsheet, word processor, image, etc.). Do not store confidential data on transportable electronic media.

Electronic media must be purged, degaussed, or otherwise destroyed so the data cannot be restored.

Paper records:
Do not send or receive complete bank account or credit card numbers using email or campus mail.
Never ask for the pin or credit card security code unless the cardholder is on the phone and the code is immediately entered directly into the on-line hosted software. Never write down the pin or security code.

Avoid retention of paper records containing complete bank account or credit card numbers. If, for business reasons, you must store full account/card numbers, after 36 months dispose of these records via confidential recycling, cross-cut shredding, or incinerating. Records containing partial card numbers should be retained no longer than seven years. Mark these records as confidential with a disposition date. Types of records include registration payment documents, admission applications, and credit card charge back notifications from Elavon Merchant Payment Systems.

Storage containers for recycling must be secure (locking and with document-only sized openings).
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.

If paper records are retained for a valid business purpose, physically secure the records containing full bank account or credit card numbers in locked cabinets or offices with adequate key control. Inventory of keys and/or pass code access must be performed annually. Inventory paper records containing full or partial bank account or credit card numbers periodically, minimally once per year, to identify loss or theft of items.

PCI Compliance Procedures 200.080cd

Staff Access:
Staff access rights are limited to the least privileges necessary to perform the assigned job functions. Assignment of privileges is based on job classification and function. The department manager will request staff access and privileges. Hosted solutions must include access controls that support user roles based on job function. SOU payment application security officers will review all user access and profiles/roles at least annually.

Users are required to log off payment web sites or initiate a password-protected screen saver when leaving their PC. Passwords are unique to each user. First-time users receive a unique password and must change it on their first sign-in. Passwords may not be shared; group passwords are prohibited. Before resetting passwords, the security officer may verify the users' identity via appropriate means. Accounts that have not been accessed for 90 days are subject to inactivation. Users are required to report the loss of passwords to the security officer as soon as the loss is discovered.

Users will report any suspected tampering of websites or card processing devices including PCs and laptops to the appropriate security officer. Tampering can include new devices attached to hardware, unusual or new log in requirements, and other user credentials saved on the device or software. All users should be minimally trained to recognize signs of tampering.

Terminated employees are required to turn in keys, and the manager of each department and/or the security officer of the hosted payment site should de-activate pass codes within 24 hours or the next business day.

Processing devices or hosted software:
Request an OST approved credit card device and merchant account from Business Services. These devices operate as analog and not Voice Over IP. Departments may request a CashNet Emarket for recurring events or sales. An Emarket does not require use or purchase of special devices, application for a merchant account, or new or additional state approval.

Hosted software must be approved by the Compliance Manager of OST before contracts are signed. Potential service providers are required to submit the state 3rd Party Qualification questionnaire. If the service provider cannot meet the standards set by OST, the software cannot be purchased or used. Members of the project team selecting new software must include network security and compliance staff of Information Services and Business Services.

The contract must include an acknowledgement that the service provider is responsible for the security of the cardholder data they possess, store, process or transmit on behalf of the customer. See 12.8.2 of the Coalfire One quality assurance questionnaire.

Annually, Business Services will review the service providers to determine their status as PCI-DSS compliant. If a service provider is no longer compliant, OST will be contacted for assistance in evaluating and determining steps to mitigate risk and establish a business continuity plan that would allow temporary use of the service provider. Business Services, I.T. and the user department personnel form the review committee that addresses internal and external processes. See 12.8.4.

Oregon law requires that state funds are deposited directly into a recognized Oregon depository within one business day. For this reason the use of PayPal or similar services that do not deposit proceeds directly into an OST merchant account are prohibited. See ORS 293.265.

Training:
All staff will be trained in the policy when first allowed access to process or manage sensitive data. Staff are expected to review the policy when business processes change, and work with Information Technology and Business Services to design the appropriate security revisions.

Contractors are covered by this policy.

Data Security and Incident Response:
The Senior Vice President of Finance and Administration will assign security and policy responsibilities to the CIO and the Director of Business Services. They will develop security policy and procedures, monitor and analyze security alerts, develop, distribute and test the incident response and escalation procedures, perform administration of user accounts, and monitor and control all access to data.

Electronic security breaches are reported as soon as the event is discovered, to the Chief Information Security Officer. See the Incident Response Plan at https://inside.sou.edu/it/it-policies.html. The Director of Business Services functions as liaison to OST and can perform steps to report or mitigate loss and prepare follow up responses for the bank and/or law enforcement inquiries.

D. Appendix

OST PCI security policies - go to
http://www.oregon.gov/treasury/Divisions/Finance/StateAgencies/Pages/Policies.aspx:

- 02.18.13 Data Security
- FIN 214 Third Party Vendor Requirements
- Third Party Vendor Application

SOU Information Technology Security Policy

- https://inside.sou.edu/assets/policies/docs/FAD040-information-security.pdf
- https://inside.sou.edu/assets/it/docs/incident-response-plan.pdf

User Data Security Verification Statement – see page 5

User Data Security Verification Statement

I have received a copy of the SOU PCI Compliance Policies and Procedures and have read and understand the policy. I agree to observe the terms and conditions of this policy.

In addition and if applicable: I have read and understand the requirements set forth by the Information Security Policy no. FAD.040, related to the protection, use, processing, storage, communication and transmission of data used in electronic commerce.

Signed Name _____

Printed Name _____

Organization _____
(SOU department or vendor organization name)

Date: _____

Please return to the Associate Director, Business Services.