OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

212 PAYMENT CARD INFORMATION SECURITY REQUIREMENTS

SUBJECT:	PAYMENT CARD INFORMATION SECURITY REQUIREMENTS
NUMBER:	212
AUTHORIZING BODY:	VICE PRESIDENT FOR FINANCE & ADMINISTRATION
RESPONSIBLE OFFICE:	CONTROLLER'S OFFICE AND UNIVERSITY TECHNOLOGY SERVICES
DATE ISSUED:	JULY 2005
LAST UPDATE:	AUGUST 2018

RATIONALE: Oakland University (University) is subject to rules, regulations, and contractual provisions regarding the handling of Payment Cards and Cardholder Information, as those terms are defined below. This Policy provides mandatory security measures and procedures for University Departments (Departments) accepting Payment Cards for payment.

POLICY: Departments must adhere to the following security measures and University procedures to maintain security of Payment Cards and Cardholder Information, and to ensure the University remains eligible to accept Payment Card payments. Failure to comply may subject the University to severe penalties.

SCOPE AND APPLICABILITY: Any Department that accepts Payment Cards as a payment method must adhere to Policy 212.

DEFINITIONS:

Cardholder Data Environment: the devices, systems, applications, and networks identified as in scope of Payment Card Industry Compliance.

Cardholder Information: Card holder's name, contact information, Payment Card number, the Primary Account Number, card expiration date, Payment Card Validation Code, Payment Card transaction information, or any other information that may be used to personally identify a Payment Card account or holder.

Media Access Control address (MAC address): a unique identifier assigned to network interface controllers for communications at the data link layer of a network segment.

Payment Card: credit cards, debit cards, ATM cards, and any other card or device other than cash or checks, issued by a bank or credit union that is normally presented by a person for the purpose of making a payment.

Payment Card Industry (PCI) Compliance: compliance with the standards set forth by the PCI Security Standards Council.

Payment Card System: any computing or information technology device, server, desktop computer, mobile device, software application, hosted service, software-as-a-service (SaaS), app, multi-function device, or other system or technology used to process, transmit, or store Cardholder Information.

Payment Card Validation Code: sometimes referred to as the CVV, CV2, or CVV2 codes, the validation code is the three digit value printed on the signature line on the back of the Payment Card, or the four-digit code located on the front of certain Payment Cards.

Primary Account Number: Card identifier found on payment cards, such as credit cards and debit cards, as well as stored-value cards, gift cards and other similar cards. In some situations the card number is referred to as a bank card number.

PROCEDURES:

1. Payment Card Systems

   University Technology Services (UTS) will define, document, and manage the Cardholder Data Environment. Payment Card Systems must be installed and verified by UTS. A Payment Card System must be protected by a firewall installed and maintained by UTS. UTS will perform a complete network and systems review for verification of Cardholder Information security prior to any Payment Card System being used to process, transmit or store Cardholder Information. Before implementing any changes to a Payment Card System, UTS must authorize, formally document, plan and log the changes.

2. Communications

Sending Primary Account Numbers by end-user messaging technologies (i.e. email, instant messaging, chat, etc.) is strictly prohibited.

All transmissions over public networks of Cardholder Information must be encrypted through the use of SSL or other industry acceptable methods, using the latest standards as identified by UTS.

Remote access to a Payment Card System must be encrypted and secured by UTS; no other remote access is allowed.

3. Device Management

All devices must be labeled with owner, contact information and purpose. Additionally, the device's MAC address must be documented and provided to UTS if attached to the network.

All workstations, information technology devices, and all other components that are part of a Payment Card System must have anti-virus software installed, current anti-virus definitions, current operating system and patches installed. Local firewalls, strong passwords, system and network logs, and password protected screen savers must be enabled.

Server-based Payment Card Systems must be managed by UTS and must be maintained in compliance with Administrative Policy 880, Systems Administration.

Student Business Services is responsible for the annual review of the vendors / processors Service Organization Controls reports or a similar document that verifies the service delivery processes and controls of the Organization. The results of all review(s) are reported to UTS and the Controller's Office.

Point of Sales devices must be reviewed and approved by Student Business Services and UTS. Device purchases, maintenance, and security updates will be managed by Student Business Services. Devices will be purchased from the University’s approved Payment Card processor whenever possible; if not possible, Student Business Services will identify an approved alternative.

Payment Card Industry Security Standards Council requires that the University securely maintain Payment Card devices used in card present transactions (that is, card swipe or dip) at the point of sale by:

- Maintaining a list of devices
- Periodically inspecting devices to look for tampering or substitution

- Examining the list of devices to verify the list includes
    - Make, model of device
    - Location of device (for example, the address of the site or facility where the device is located)
    - Device serial number or other method of unique identification.
- Selecting a sample of devices from the list and observing device locations to verify that the list is accurate and up to date.
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices
- Examining documented procedures to verify processes are defined to include the following:
    - Procedures for inspecting devices (maintained by Student Business Services
    - Frequency of inspections

Departments are responsible for inspecting their Payment Card devices at least monthly. Departments are required to log the results of their inspection(s) on a "Swipe Terminal Inventory Sheet and Tampering Checklist" provided by Student Business Services. Departments are required to include the device inspection process in their departmental procedures. The results of all inspections will be reviewed by Student Business Services periodically.

Student Business Services is responsible for an annual review of the Payment Card devices and related documented procedures. The results of all review(s) are reported to UTS and the Controller's Office.

4. Payment Card Processing

Departments are required to have detailed procedures regarding Payment Card Processing that incorporate all PCI Compliance requirements. Current requirements are available from Student Business Services. Departments are required to submit a reviewed and updated copy of their internal procedures annually to Student Business Services. Departments who do not submit their updated procedures annually may have their Payment Card processing privileges revoked.

In Person:

- Only approved staff should be handling Payment Card transactions.
- Departments must review the physical Payment Card presented for the following:
    i. Is the card valid? The card may not be used after the last day of the expiration month embossed on the card.
    ii. Only the actual card/account holder should be using the card.
    iii. Does the customer's signature on the charge form match the signature on the back of the card? Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.
    iv. Does the signature panel on the card look normal? Check to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.
    v. Does the account number on the front of the card match the number on the back of the card and the terminal receipt display? If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.
    vi. Does the name on the customer receipt match the embossed name on the front of the card? If the name is different, this could indicate an altered card.
- Retain the signed merchant copy of the swipe machine-generated receipt and return the other copy to the Cardholder.
- Place the merchant copy of the receipt in a secure, limited access area until taken to the University’s Cashier’s Office.
- Departments are not permitted to key in a Payment Card transaction when the physical card is present. If the Payment Card transaction will not process through the Point of Sale device, ask for another payment method or ask the customer to pay online (if applicable).

If you are suspicious of a Payment Card transaction, contact the Voice Authorization Center and request a Code 10 Authorization. Using the

term “Code 10” allows you to call the Voice Authorization Center to question the transaction without alerting the Cardholder.

To request a Code 10 Authorization for a Discover Network, Visa, MasterCard, or American Express Transaction, call the telephone number on the Voice Authorization sticker (located on the Point of Sale Device).

Follow the instructions given to you on how to proceed by the processor.

Paper Format or Other Hard Copy / Mail:

- Every effort must be made to avoid using a paper format or other hard copy / mail to obtain Cardholder Information.

- All paper formats and other hard copy instruments to collect Cardholder Information must be reviewed and approved by Student Business Services.

- Cardholder Information in paper format or other hard copy must be stored in a secure, limited access area until processed. Once the payment is processed, the portion of the form or other hard copy that contains Cardholder Information must be securely shred in a cross cut / confetti shredder. Departments have no need to maintain a paper copy of Cardholder Information.

- Place the merchant copy of the receipt in a secure, limited access area until taken to the University’s Cashier’s Office.

Fax:

- In general, business operations handling a high volume of Payment Card transactions should plan out business processes that do not accept Payment Cards by fax. Business processes designed to accept occasional payment cards by fax must be reviewed and approved by Student Business Services in advance.

- The fax machine must be located in a secure area not accessible to the public.

- Use of a multi-function printer / fax machine increases the PCI scope of the University; a plain paper, dial up fax is recommended.

- Faxes with payment information must be immediately distributed to the individual responsible for key-entering the information into the approved swipe device or payment application.

- The fax containing Cardholder Information must be stored in a secure, limited access area until processed. Once the payment is processed, the portion of the form or other hard copy that contains Cardholder Information must be securely shred in a cross cut / confetti shredder. Departments have no need to maintain a paper copy of Cardholder Information.

- The customer copy (with redacted Cardholder Information) may be faxed, mailed, or emailed to the customer (optional).

- Place the merchant copy of the receipt in a secure, limited access area until taken to the University's Cashier's Office.

Telephone:

- In general, business operations handling a high volume of payment cards should plan out business processes that do not accept Payment Cards over the phone. Business processes designed to accept occasional Payment Cards by phone must be reviewed and approved by Student Business Services in advance.

- If Cardholder Information must be written down, it should be processed immediately after the call has concluded.

- Once the payment is processed, the portion of the form or other hard copy that contains Cardholder Information must be securely shred in a cross cut / confetti shredder. Departments have no need to maintain a paper copy of Cardholder Information.

- Place the merchant copy of the receipt in a secure, limited access area until taken to the University's Cashier's Office.

- Do not accept payment information via a voicemail or phone message.

Email:

- Do not accept payment Cardholder Information via an email. Open communication systems such as email or chat programs are not considered secure for the transmission of any Cardholder Information. If a client should send their payment information to the department, the following steps should be taken:

a. Click “Reply” on the email
b. Delete the payment card data from the original portion of the email.
c. In your response, Copy and paste the following
    i. “Thank you for contacting (insert department or name). We appreciate your business, however as part of our compliance effort with the Payment Card Data Security Standard and our practice to protect all of our customers’ Personally Identifiable Information, we cannot process the payment that you have sent through email. We ask that you use one of the following approved methods for making your payment:
        - Online – www.xxxxxxxxxx.edu
        - Mail – mailing address
        - Phone – xxx-xxx-xxxx
        - Fax – xxx-xxx-xxxx
    ii. Then promptly delete the original email and empty the trash.

5. <u>Storage and Disposal</u>

a. Banking regulations require an original draft or a legible copy of Payment Card transaction receipts be retained for 18 months from the date the transaction took place. Sales slips / receipts must be turned in to the University’s Cashier’s Office with the department’s daily deposit for proper storage and disposal using a cross cut / confetti shredder.
b. Cardholder Information must not be stored in any Cardholder Data Environment or any Payment Card System.
c. Storage of the full contents of any track from a Payment Card magnetic stripe, whether on the back of the Payment Card, in a chip or otherwise, is strictly prohibited.
d. Access to areas used to process, transmit or store Cardholder Information must be restricted to authorized University personnel on a need-to-know basis. ID badges, office keys or comparable security devices must be used to restrict access.

    i. Portable Point-of-Sale devices (includes terminals, PIN pads, etc.) must be secured in a locked cabinet, locked drawer or a safe when not in use.

    ii. Cash registers must be protected with a password screen lock when not in use.

    iii. All Payment Card information and Cardholder Information must be removed from a University employee’s work area if that

University employee is not physically present at the workstation.

e. Departments' Point of Sale devices must be settled daily and cleared after settlement.

f. Departments who need to dispose of a Payment Card System must notify Student Business Services and UTS before proceeding. Disposal of a Payment Card System must be handled through University Property Management and must be accompanied by the computer release form which can be found on the Property Management website. The release must be compliant with Administrative Policy #880, System Administration Responsibilities and the Payment Card System must be formatted and cleaned such that any residual data, Cardholder Information, or software application cannot be retrieved.

6. Public Display & Disclosure

All but the last four digits of the Payment Card account number must be masked or black-lined whenever any other Cardholder Information is displayed.

Cardholder Information should not be verbally repeated in front of anyone other than the Payment Card holder.

All Cardholder Information must be restricted and/or blocked from the view of third-party customers and others without the need to know. Glare screens or similar devices may be used to restrict or block the view of others.

7. Access

Background checks for employees with access to processing, transmission or storage of Cardholder Information will be performed in accordance with Administrative Policy 725, Filling Vacancies (Excluding Academic).

Employees with access to processing, transmission or storage of Cardholder Information must attend and acknowledge annual training for this policy and Policy 210 Cash Receipts. Student Business Services is responsible for providing this training and logging attendance. Departments who do not participate in annual training may have their Payment Card processing privileges revoked.

Access to a Payment Card System must be protected by secure login and password, and must be restricted to those with a need to know. Departments that accept Payment Card payments electronically must also follow Administrative Policy 860, Information Security. Authorization for Departments

to accept Payment Card payments must be obtained in advance of process creation from Student Business Services.

Employee access must be removed immediately upon termination of employment.

Access provided to any individual who is not a University employee, such as contractor or temporary employees, must be reviewed in advance by Student Business Services and UTS.

Vendor access must be enabled only for the duration of need and disabled immediately upon completion of service.

Group, shared or generic access to a Payment Card System or Cardholder Information is strictly prohibited.

Prior to sharing Cardholder Information with an external organization, or entering into an arrangement with a vendor to process Payment Card transactions, a written agreement must be reviewed and approved in advance by Student Business Services and UTS.

8. Security Incidents

Any release or exposure of Cardholder Information to an unauthorized third party, or unauthorized access to a Payment Card System must be reported to UTS, Student Business Services and the Controller's Office. Reports and emergency response will be processed under provisions described for Confidential Data in Policy #860 Information Security.

9. PCI (Payment Card Industry Compliance)

The University participates and complies with the standards set forth by the PCI Security Standards Council (PCI SSC) which requires annual validation of the University's operation within the PCI Compliance standards. Departments must facilitate the validation process by timely providing accurate information requested by Student Business Services and UTS.

PCI Security Standards Council also requires the University's payment application provider(s) to annually certify that the payment application meets certain industry standards for data security (Payment Application Data Security Standards).

Oakland University requires the actual PCI Compliance certificate from the vendor and processor before a system is approved or renewed. Student Business Services is responsible for keeping approvals and renewals of certificates of compliance related to PCI Compliance and Payment Application

Data Security Standards. Student Business Services is responsible for the annual review of the PCI Security Standards Council's website to be sure the vendor / processor is re-certifying annually.

10. Payment Card Processor Merchant Operating Guide

    The University must abide by the policies and practices established within the Merchant Operating Guide provided by the University's payment processor, which can be found on the Cashier's Office website oakland.edu/cashiers.

    Any questions regarding compliance with this Administrative Policy 212 should be directed to Student Business Services or UTS.

RELATED POLICIES AND FORMS:

OU AP&P #210 Cash Receipts

OU AP&P #860 Information Security

OU AP&P #880 System Administration Responsibilities

Cashier's Office Website