ADMINISTRATIVE POLICIES AND PROCEDURES

SUBJECT:	BANKCARD 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:	FEBRUARY 2016

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

POLICY: Departments must adhere to federal regulations and the following security measures and University procedures to maintain security of Bankcards and Cardholder Information, and to ensure that the University remains eligible to accept Bankcard payments. Failure to comply may subject the University to severe penalties.

SCOPE AND APPLICABILITY: Any department that accepts Bankcards as a payment method must adhere to Policy 212.

DEFINITIONS:

Bankcard means credit cards, debit cards, ATM cards, and any other payment 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.

Bankcard Validation Code is the three digit value printed on the signature line on the back of the Bankcard.

Cardholder Information means a Bankcard holder's name and contact information, Bankcard number, the Primary Account Number (PAN), card expiration date, security code (CVV2, CVC2, etc.), Bankcard transaction information and/or any other information that may be used to personally identify a Bankcard account or holder.

Cardholder Data Environment (CDE) is defined as the devices, systems, applications, and networks identified as in scope of Payment Card Industry compliance.

Payment Card Industry (PCI) Compliance means to comply with the standards set forth by the PCI Security Standards Council (PCI SSC).

PROCEDURES:

1. Network and Systems

University Technology Services **(**UTS) will define, document, and manage the Cardholder Data Environment (CDE). Any computing or information technology device, server, desktop computer, mobile device, software application, hosted service, or other system used to process, transmit or store Cardholder Information (Bankcard System) must be installed and verified by UTS. A Bankcard 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 Bankcard System being used to process, transmit or store Cardholder Information. Before implementing any changes to a Bankcard System, UTS must authorize, formally document, plan and log the changes.

Sending Primary Account Numbers (PAN) by end-user messaging technologies (i.e., e-mail, 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.

All workstations, information technology devices, and all other components that are part of a Bankcard System must have anti-virus software installed, current anti-virus definitions, current operating system and patches installed, and local firewalls, strong passwords, system and network logs, and password protected screen savers enabled. No remote access is allowed. All devices must be labeled with owner, contact information and purpose, or the device must be assigned a MAC address and be network attached.

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

Point of Sales (POS) devices must be reviewed and approved by Student Business Services and UTS. Device purchases will be managed by Student Business Services. Devices will be purchased from the University's approved Bankcard processor whenever possible.

2. Storage and Disposal

a. Cardholder Information in paper format or other hard copy must be stored in a secure, limited access area for a period of 18 months. **All but the last four digits of the Bankcard account number must be redacted (masked or black-lined) or truncated.** When receipts, paper and other hard copies of Bankcard information or Cardholder Information are disposed of, they must be shredded using a cross cut/confetti shredder, or a bonded, secure data disposal service.

b. Banking regulations require an original draft or a legible copy of Bankcard transaction receipts be retained for 18 months from the date the transaction took place. **All but the last four digits of the Bankcard account number must be redacted (masked or black-lined) or truncated.**

c. Cardholder Information must not be stored on any system, computing or information technology device, server, desktop computer, backup device, cloud service, hosted solution or point of sale device without prior review by UTS. Storage of Cardholder Information on mobile devices, including laptops, notebooks, USB keys or smartphones is strictly prohibited.

If permitted, storage of the Bankcard account number must be encrypted or truncated and retention limited to the time required for business, legal and regulatory requirements, but no longer than 18 months. Electronic data must be securely disposed of by crushing, degaussing, or shredding.

d. Disposal of a Bankcard 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 Bankcard System must be formatted and cleaned such that any residual data, Cardholder Information or software application cannot be retrieved.

e. Storage of the full contents of any track from a Bankcard magnetic stripe, whether on the back of the Bankcard, in a chip or otherwise, is strictly prohibited.

f. Storage of the Bankcard Validation Code is strictly prohibited.

g. 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, imprinters, etc.) must be secured in a locked cabinet or locked office when not in use.

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

iii. All Bankcard 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.

h. Departments' point of sale devices must be settled daily and cleared after settlement.

3. Display

All but the last four digits of the Bankcard account number must be masked or black-lined whenever any other Cardholder Information is displayed, regardless of whether such information appears on paper, fax, email, computer display, log files or otherwise. Bankcard account numbers must not be transmitted via email.

Departments should avoid taking Cardholder Information via cell phone.

Cardholder Information should not be verbally repeated in front of anyone other than the Bankcard 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.

4. Application and Web Development

All software application and/or web development involving the storage, processing or handling of Cardholder Information, must be created following a defined software development life cycle and commonly accepted security guidelines, such as Open Web Application Security Project guidelines, and approved by UTS prior to launch, implementation, deployment or use.

5. 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.

Access to a Bankcard System must be protected by secure login and password, and must be restricted to those with a need to know. Departments that accept Bankcard payments electronically (including without limitation, via personal computer, Internet or voice response) must also follow Administrative Policy 860, Information Security. Authorization for Departments to accept Bankcard payments must be obtained in advance of process creation from Student Business Services for point of sale processing, and from Student Business Services and UTS for electronic processing.

Employee access must be removed immediately upon termination of employment.

Access provided for any individual who is not a University employee, such as contract or temporary employees, must be reviewed in advance by the Office of Risk Management and Student Business Services.

Group, shared or generic access to a Bankcard System or Cardholder Information is prohibited.

Prior to sharing Cardholder Information with an external organization, or entering into an arrangement with a vendor to process Bankcard transactions, a written agreement must be reviewed and approved in advance by the Office of Risk Management, UTS, and Student Business Services for merchant identification.

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

6. Security Incidents

Any release or exposure of Cardholder Information to an unauthorized third party, or unauthorized access to a Bankcard System must be reported to the Office of Risk Management. If a Bankcard System was involved in such exposure, release or unauthorized access, notification must also go to UTS. An emergency response plan will be implemented as necessary.

7. PCI (Payment Card Industry) Compliance

The University participates and complies with the standards set forth by the PCI Security Standards Council (PCI SSC). PCI SSC 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 UTS.

PCI SSC also requires the University's payment application provider(s) to annually certify that the payment application meets certain industry standards (PA-DSS).

Oakland University requires the actual PCI Compliance certificate from the vendor / processor before a system is approved or renewed. UTS is responsible for keeping approvals and renewals of certificates of compliance related to PCI Compliance and PA-DSS. Student Business Services is responsible for the annual review of the Visa Compliance List to be sure the vendor / processor is re-certifying annually. Student Business Services is responsible for the annual review of the vendors / processors Service Organization Controls (SOC) 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 AVP / Controller's Office.

PCI SSC requires that the University securely maintain Bankcard 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 it 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

Student Business Services will be responsible for the annual review of the Bankcard devices and related documented procedures. The results of all review(s) are reported to UTS and the AVP / Controller's Office.

8. Bankcard 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 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