Oakland University
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:	SEPTEMBER 2006

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. Failure to comply may subject the University to severe penalties.

SCOPE AND APPLICABILITY:

DEFINITIONS:

Bankcard means 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 seeking to make payment, for the purpose of making a payment.

Cardholder Information means a Bankcard holder's name and contact information, Bankcard number, account number, card expiration date, CVV2, CVC2, Bankcard transaction information and/or any other information that may be used to personally identify a Bankcard account or holder.

PROCEDURES:

1. Storage

a. Cardholder Information must not be stored on any system, computing or information technology device, server, desktop computer, backup device, or point of sale device without prior review by University Technology Services (UTS).

b. Cardholder Information must not be stored on laptop, notebook or mobile computers at any time.

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

d. Any Cardholder Information in paper format or other hard copy must be stored in a secure, limited access area for a period no longer than is necessary to meet document retention procedures of the individual Departments. However, an original draft or a legible copy of Bankcard transaction receipts must be retained for at least 18 months from the date the Departments were paid for the transaction, subject to the restrictions set forth in paragraph 3 regarding the display of Bankcard account numbers and Cardholder Information.

e. Access to an area 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. 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.

f. 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.

g. Storage of the Bankcard-Validation-Code (the three digit value printed on the signature line of the Bankcard) is strictly prohibited.

h. If permitted, storage of the Bankcard account number must be encrypted or truncated.

2. Network and Systems

Any computing or information technology device, server, desktop computer, 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.

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.

UTS will periodically review the Departments' system logs, network logs, and backup, disaster recovery and business continuity plans. If the Bankcard System and its server are physically located within the Departments, the Departments must keep the system logs for a minimum of one calendar year.

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 given on a 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

Access to a Bankcard System must be protected by secure log-in 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 OU AP&P #860 Information Security. Authorization for Departments to accept Bankcard payments must be obtained in advance of process creation from the Controller's Office (Student Business Services) for point of sale processing, and from 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.

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.

6. Disposal

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.

Disposal of a Bankcard System must be handled through University Property Management and must be accompanied by the Computer Release Form.

The release must be compliant with OU AP&P #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.

7. 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.

8. Cardholder Information Security Program

The University participates and complies with the standards set forth by the Visa U.S.A. Cardholder Information Security Program ("CISP"). CISP requires annual validation of the University's operation within the compliance standards. Departments must facilitate the validation process by timely providing accurate information requested by UTS.

UTS will be responsible for keeping certificates of compliance related to CISP and for requesting annual updates to such certificates.

9. Any questions regarding compliance with this OU AP&P #212 Bankcard Information Security Requirements should be directed to the Controller's Office, Student Business Services or University Technology Services.

RELATED POLICIES AND FORMS:

OU AP&P #210 Cash Receipts

OU AP&P #860 Information Security

OU AP&P #880 System Administration Responsibilities

APPENDIX:

 Return to Table of Contents