MEMORANDUM

DATE: June 27, 2007
TO: Oakland University Faculty and Staff
FROM: Issued Jointly by the Controller's Office, Purchasing and Risk Management, and University Technology Services

SUBJECT: Credit and Payment Card Information Security and PCI

Compliance

You may be aware of the privacy concerns surrounding the business practice of storing credit card information electronically, particularly on personal computers, servers and other storage devices. This privacy concern also applies to storing credit card information in any form, including paper files.

The payment card industry (American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International) created a set of security standards to protect their customers from increasing identity theft and security breaches. This set of security standards is called Payment Card Industry (PCI) compliance. Oakland University is required to be PCI compliant because the university accepts, processes, transmits or stores credit card information. If Oakland University contracts with a vendor or service provider to accept, process, transmit or store credit card information, the vendor also is required to be PCI compliant.

If your department or operation is considering the purchase of a system that will accept, process, transmit or store credit card information, such as credit card payment on a Web site or other similar processes, you first need to review critical university policies:

#212 Bankcard Information Security Requirements – **http://www2.oakland.edu/audit/POLCY212.HTM**

#860 Information Security – **http://www2.oakland.edu/audit/POLCY860.HTM**

#870 Software Regulations – **http://www2.oakland.edu/audit/POLCY870.HTM**

Key points to remember:

- The Office of Purchasing and Risk Management must provide advance review and approval of contracts, purchase agreements and licenses for the acquisition of software that either (1) costs $2,500 or more, (2) requires a site license or site license agreement, or (3) handles confidential data, such as defined under PCI compliance, as defined in University Policy **#860 Information Security**.
- Before contacting Purchasing and Risk Management about a contract or purchase requisition, the unit needs to review and specifically identify the data elements that will be sent to a vendor (including all personal information, such as name, address, Social Security Number, and Grizzly ID number).
- ASP is a technology solution or system where a third party manages and distributes software-based services and solutions, including data storage, appropriate to that software solution, to customers across a wide area network from a central data center. These are usually Web-based solutions where data is sent to off-campus systems and accessed via the Internet. Such systems may provide the ability to accept payment over a Web site. Departments employing ASPs must consult with the General Counsel's Office and/or the Office of Risk Management prior to contract.
- 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).
- 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.
- If your department or operation already has a system that will accept, process, transmit or store credit card information, such as credit card payment on a Web site or similar process, you need to request and keep a copy of the PCI compliance certificate, and provide a copy to UTS, annually.
- Bankcard account numbers must not be transmitted via e-mail.
- Protection of cardholder information applies to paper as well as electronic storage.

UTS-1655 8/07

Oakland UNIVERSITY

Questions about payment card processing should be directed to Linda Switzer at **switzer@oakland.edu**.

Technology questions should be sent to Terrie Rowe at **rowe@oakland.edu**.