



WICHITA STATE UNIVERSITY

Audit Update

A Newsletter from the
Office of Internal Audit
201 Morrison Hall, Campus Box 205

Director of Internal Audit
Chris Cavanaugh 5823

Senior Internal Auditor
Terry Coltrain 5824

Summer 2009

Security of Credit Card Data

In January 2009, the University adopted **Section 13.14 of the *WSU Policies and Procedures Manual, Security of Credit Card Data***. The purpose of the policy is to establish the University's intent to comply with the Payment Card Industry Data Security Standard (PCI DSS).

In 2006, a consortium of payment card companies formed the Payment Card Industry Security Standards Council (PCI SSC), an independent body to promote the adoption and global management of PCI DSS. The primary objective of PCI DSS is to protect the personal information of cardholders' data.

Compliance with PCI DSS is required of all merchants that process, store, or transmit cardholder data. This definition of "merchant" includes most all colleges and universities. Though PCI DSS compliance is contractually required, it also reflects good business practice. The financial costs of a data breach can be significant, but these costs may pale in comparison to the reputational cost incurred should the University violate the trust of students, parents, and alumni.*

* Walter Conway and Dennis W. Reedy discuss this in-depth in the December 2007 issue of *Business Officer* published by the National Association of College and University Business Officers.

Policy Statement

Section 13.14 contains the following provisions (refer to the *WSU Policies and Procedures Manual* for the full text):

1. The Director of Financial Operations, or the Director's designee, shall approve each department or unit requesting to accept credit cards.
2. All transactions that involve the transfer of credit card data must be performed on systems provided or approved by the University for this purpose.
3. No credit card numbers or documentation containing credit card numbers or cardholder data shall be transmitted or stored in any personal computer or email account.
4. No paper documents, including, but not limited to, paper receipts and hand-written notes, containing credit card numbers or cardholder data shall be stored by an approved department or unit.

Credit Card Information Security Procedures

To assist with compliance with PCI DSS and the University's Security of Credit Card Data Policy, the **Office of Financial Operations and Business Technology** has adopted the procedures detailed in the adjoining column.

For these procedures, "credit card information" refers to a cardholder's number, expiration date, PIN, and the 3 or 4 digit number on the back of the card.

Collection

- Collection of credit card information over the **phone or through mail** is discouraged, but permitted, if all other procedures as set forth below are followed.
- Collection of credit card information through **electronic mail** is not permitted.
- Collection of credit card information using an **electronic fax machine** is discouraged, but permitted. The fax machine should be accessible only to department staff.

Access and Transportation

- **Access** to credit card information should be limited to department employees on a "need-to-know" basis.
- **Transportation** of credit card information should be limited to employees who have regular access to the information, or to employees who have been approved by the Office of Financial Operations.

Storage

- **Electronic storage** of credit card information is not permitted under any circumstances.
- **Temporary physical storage** – Any document containing credit card information must be stored in a locked cabinet or file until the information can be transported to Financial Operations.
- **Permanent physical storage** of credit card information in campus departments is not permitted. Documents or forms used to collect credit card information for payment processing must be
 - destroyed (shredded) in their entirety, or
 - the credit card information must be physically removed (*i.e.* cut out or off) from the document or form within two business days.

Campus Departments Using Credit Card Terminals

- Credit card terminal transactions shall be settled at the end of each business day.
- All credit card terminal receipts from the terminal's daily settlement shall be transported to Financial Operations within two business days of the credit card transaction.
- The physical location of the credit card terminal must be accessible to departmental staff only.

Campus Departments Not Using Credit Card Terminals

- All credit card information collected by a campus department must be transported to Financial Operations within two business days.