

Subject: PCI DSS Policy	Author: Controller' s Office/Treasury Dept.
Effective Date: February 1, 2010	Last Review Date:
Last Revision:	Revised By:
Contact Name: David M. Woods	Contact Email: treasmgt@louisville.edu
Approved By: Larry Zink	Page 1 of 2

University of Louisville has an obligation to protect sensitive financial information, such as credit card data, of the University's customers. That is what PCI DSS is about. Due to growing consumer concerns over compromised credit card data, the five major credit card associations (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa) joined forces to establish a security program for merchants called the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS is a compliance initiative that dictates security standards for merchants and service providers for the safe handling of credit card information. Without compliance, the card industry may refuse to allow you or the University as a whole, to process credit cards and/or hefty fees and fines could be charged for noncompliance. **Therefore, every UofL office that accepts credit cards must become PCI DSS compliant.**

All departments accepting credit cards should be familiar with the risks, fees, and security requirements involved with being a credit card merchant. This means any card (credit, debit, prepaid, stored value, gift or chip) bearing the logo of one of the PCI Security Standards Council's five founding payment brands is required to be protected as prescribed by the PCI DSS. All University merchants must validate their PCI-DSS compliance by completing an annual PCI DSS Self Assessment Questionnaire (SAQ). Treasury Management will determine which SAQ ([A](#), [B](#), [C](#) or [D](#)) you need to complete and forward it to your Merchant Department Responsible Person (MDRP) designated for your Merchant Account. Periodically a vulnerability scan of the network will be conducted by the University.

Your department can assist in achieving and maintaining compliance by adhering to the following:

- All systems that process credit cards require approval by Treasury Management with consultancy from Information Technology.
- Departments must contact Treasury Management before entering into any contracts for software and/or equipment related to credit card processing.
- If Virtual Merchant (internet based) is used as the method of processing, a dedicated workstation is required whose **internet access is limited to credit card processing only**. A custom Firewall must be installed for the workstation by the University's Information Technology department. While the University has a global firewall protecting Merchants to an extent from threats outside the University, an additional firewall is needed to protect from attacks inside the University. A one-time setup fee and annual fees will be incurred with this method. Current pricing can be found on the [Application for a New Merchant Account](#). Surplus equipment would require IT review has having updatable characteristics.
- If a Credit Card Terminal Swipe Machine is used a dedicated phone/fax line is required.
- All computers that process credit cards must use a desktop. If a laptop dedicated to credit card processing must be used, wireless capability must be disabled.
- Departments must not maintain sensitive credit card data such as credit card numbers, card type, expiration date, PIN, and card validation codes and/or any magnetic strip data.
 - Credit card or personal payment information shall never be downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.

- The three digit card validation code (CV2, CVC2) printed on the signature panel of a credit card and/or any magnetic strip data shall never be stored in any form.
- If it is necessary to display credit card data, all digits except the last four digits of any credit card account number shall always be masked.
- If it is necessary to maintain physical records, documents containing credit card and/or personal payment data shall be securely stored in a locked file cabinet.
- All physical and electronic credit card and personal payment data that is no longer deemed necessary or appropriate to store must be properly destroyed or rendered unreadable.
- Each department maintaining a Merchant Account must complete an annual self assessment questionnaire.

When cardholder data is shared with a third party processor/ service provider (i.e., [CyberSource](#)) on behalf of the department, they must also be in compliance with PCI DSS. The department needs to ensure there is a contractual obligation for that third party processor/service provider to adhere to the PCI DSS standard and that the third party processor/service provider is responsible for the security of the cardholder data it possesses. Proof of PCI DSS compliancy by the third party processor/service provider must be provided to Treasury Management.

All campus merchants, whether they conduct e-commerce, mail-order/telephone-order, or card present transactions, are required by the University to comply with PCI DSS. Non-compliance with these standards puts the University at risk for:

- Large monetary fines assessed to your department and/or University of Louisville.
- Loss of merchant status for department.
- Loss of merchant status for University of Louisville.
- Significant increase in reporting requirements affecting the department and/or University wide.

Any fines and/or penalties associated with non-compliance and/or confirmed security breaches are defined by each of the payment card brands. Liability for a breach is accepted by the Merchant Department should a breach occur due to negligence of the department to adhere to the University's policies and procedures for [Credit Card Merchants](#).

The following are some useful links to learn more about the PCI DSS standards:

- PCI DSS – [Questions and Answers](#)
- [PCI Security Council](#)
- [Straight Talk about Data Security](#), (PDF) by Walter Conway and Dennis Reedy, Business Officer, December 2007.
- [Cards at School, Why Banks View Campuses as High Risk Customers](#), (PDF) Dennis Reedy and Walter Conway, AEP Exchange, March 2007.
- [VISA](#)
- [MasterCard](#)
- [Discover](#)
- [American Express](#)

WARNING: Some Web sites, to which these materials provide links for the convenience of users, are not managed by the University of Louisville. The University does not review, control, or take responsibility for the contents of those sites.