**Lehigh University Policy for Accepting Credit Card Payments**

Contents:

* [**Background and Purpose**](http://finance.tufts.edu/treasury/?pid=6#background)
* [**Applicability**](http://finance.tufts.edu/treasury/?pid=6#appl)
* [**Policy Statement**](http://finance.tufts.edu/treasury/?pid=6#pol)
* [**Process to Implement Acceptance of Credit Card Payments**](http://finance.tufts.edu/treasury/?pid=6#proc)
* [**Process for Responding to a Security Breach**](http://finance.tufts.edu/treasury/?pid=6#sec)
* [**Ongoing Policy Management**](http://finance.tufts.edu/treasury/?pid=6#man)
* [**Related Links**](http://finance.tufts.edu/treasury/?pid=6#rel)

**Background and Purpose**

Lehighs’ acceptance of credit cards to pay for gifts, goods and services has been growing over the past several years. Increased interest in accepting payments over the Internet (eCommerce) has also grown, spurring the need to establish business processes and policies that protect the interests of the University and its customers.

While the costs for accepting credit card payments can be significant (1.5-3.5% of every transaction, depending on the card type), it often makes sense to accept this type of payment for business reasons, which include control of receivables, competitive position and efficient processing. To the extent that it makes economic sense to do so, the University would like to support this activity. In order to ensure that credit card activities are consistent, efficient and secure, the University has adopted the following policy and supporting procedures for all types of credit card activity transacted in-person, over the phone, via mail or the Internet. This policy provides guidance so that credit card acceptance and eCommerce processes comply with the Payment Card Industry Data Security Standards (PCI DSS) and are appropriately integrated with the University’s financial and other systems.

Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, added compliance costs, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept credit card payments.

Lehigh has contracted with a third-party vendor (“Authorized Vendor,”) whose core business includes the support and processing of eCommerce transactions. The Authorized Vendor will provide the University with a secure gateway and hosted solution in which all credit card and personal payment information is transmitted to and stored on off-site computers which the Authorized Vendor owns and maintains. The Authorized Vendor must maintain PCI DSS compliance certification. This relationship will enable the University to leverage the volume of eCommerce transactions and reduce processing costs.

**Applicability**

Any Lehigh University employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit card and eCommerce payments for the University is subject to this policy. Failure to comply with the terms of this policy may result in disciplinary actions and could also limit a department’s credit card acceptance privileges.

**Policy Statement**

Any department accepting credit card and/or electronic payments on behalf of Lehigh University for gifts, goods or services (“Merchant Department”) must designate an individual within that department who will have primary authority and responsibility for eCommerce and credit card transaction processing within that department. This individual will be referred to in the remainder of this policy statement as the Merchant Department Responsible Person or “MDRP”.

All MDRPs must:

1. Execute on behalf of the relevant Merchant Department the Process to Implement Acceptance of Credit Cards for Payment detailed below.
2. Ensure that all employees (including the MDRP), with access to payment card data within the relevant Merchant Department acknowledge on an annual basis and in writing that they have read and understood this Policy for Accepting Credit Card and Payments. These acknowledgements should be submitted, as requested, to the Assoc. Treasurer.
3. Ensure that all credit card data collected by the relevant Merchant Department in the course of performing Lehigh University business, regardless of how the payment card data is stored (physically or electronically, including but not limited to account numbers, card imprints, and Terminal Identification Numbers (TIDs)) is secured. Data is considered to be secured only if the following criteria are met:
	* Only those with a need-to-know are granted access to credit card and electronic payment data.
	* Email should not be used to transmit credit card or personal payment information. If it should be necessary to transmit credit card information only the first and last four digits of the credit card number can be displayed.
	* Credit card or personal payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
	* Fax transmissions (both sending and receiving) of credit card and electronic payment information occurs only on those fax machines whose access is restricted to just those individuals who must have contact with payment card information in order to do their jobs.
	* The processing and storage of personally identifiable credit card or payment information on University computers and servers is prohibited. Exceptions can only be made if the processing and storage methods are compliant with this policy, the Lehigh University Information Technology Security Policies and PCI Data Security Standards. These standards detail strict encryption protocols.
	* Only secure communication protocols and/or encrypted connections to the Authorized Vendor are used during the processing of eCommerce transactions.
	* The three-digit card-validation code printed on the signature panel of a credit card is never stored in any form.
	* The full contents of any track from the magnetic stripe (on the back of a credit card, in a chip, etc.) are never stored in any form.
	* All but the first and last four digits of any credit card account number are always masked, should it be necessary to display credit card data.
	* All media containing credit card and personal payment data that is no longer deemed necessary or appropriate to store are destroyed or rendered unreadable.

No Lehigh University employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting business on behalf of Lehigh University may sell, purchase, provide, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction to any third party other than to Lehigh University’s acquiring bank, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request. All requests to provide information to any party outside of your department must be coordinated with the Assistant Treasurer.

Merchant Departments must use the services of the Authorized Vendor to process all eCommerce transactions. If a department believes that it has a significant business case or processing requirement that cannot be achieved using the services of the Authorized Vendor and wishes to utilize an alternative, it must initiate its request to the Assistant Treasurer.

**Process to Implement Acceptance of Credit Card and eCommerce Payments**

The MDRP or his/her designee must follow the steps below in order to implement payment card processing and eCommerce at Lehigh.

1. Complete the Lehigh University Payment Card Merchant Agreement. (For an application click [here](http://finance.tufts.edu/treasury/downloads/merchant_dept_application.doc) ). Applications must be signed by the MDRP as well as the school/division Budget or Fiscal Officer.
2. Submit the application for review and approval to the Associate Treasurer. Allow 2-3 weeks for processing of the request.
3. If the application is approved, the Associate Treasurer will provide the requesting department any necessary equipment and training.

**Ongoing Policy Management**

* Lehigh University may modify this policy from time to time as required, provided that all modifications are consistent with Payment Card Industry Data Security Standards then in effect.
* The Associate Treasurer is responsible for initiating and overseeing an annual review of this Policy, making appropriate revisions and updates and issuing the revised policy to appropriate Merchant Departments. The review will include reconfirmation of certified PCI compliance of Lehigh’ third party vendors that accept credit card payments on behalf of the University.

**Related Documents**

Lehigh University Payment Card Merchant Agreement

Guidelines for Assessing Convenience Fees

Data Security

Definitions

The web site for the PCI Security Standards Council: <https://www.pcisecuritystandards.org/>