PAYMENT CARD POLICY AND PROCEDURES

OVERVIEW

Lehigh University takes the responsibility of protecting cardholder data very seriously and is committed to maintaining compliance with the Purchase Card Industry Data and Security Standards (PCI DSS). All departments currently accepting payment cards are required to actively work with the Treasurer's Office to ensure compliance to PCID SS.

Any Lehigh University employee, contractor or agent that process, transmit, and interact with payment card data are subject to university policies as well as the data security standards as laid out by the (PCI) Security Standards Council. Security breaches can compromise a cardholder's confidential information and result in serious consequences for the university.

Lehigh has contracted with PCI DSS certified vendors, Heartland and Elavon, to process payment card information. They ensure all payment data is secure with three layers of protection (EMV Chip, encryption and tokenization) to protect issuers, merchants and consumers against fraud. There is a processing fee for this service which is charged to the departmental index.

POLICY:

Every department accepting payment card transactions on behalf of Lehigh University must designate an individual who will have primary authority and responsibility for all credit card transaction processing within the department. This individual will be referred to as the **Merchant Department Responsible Person** or **"MDRP"**.

Role of MDRP:

1. Complete a **Payment Card Merchant Agreement** ("Agreement") form (annually).
2. Ensure annually that all employees (including the MDRP), with access to payment card data within the department complete **PCI Compliance Training** and sign the **Payment Card Security Awareness Acknowledgement**. These acknowledgements must be submitted to the Treasurer's Office with the Agreement renewal.
3. Ensure that all credit card data collected by the department in the course of performing Lehigh University business 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 never be used to transmit credit card or personal payment information. If it is necessary to send detail over email it must be encrypted or only the first and last 4 digits of the credit card number may be displayed.
    - Credit card or personal payment information is never downloaded onto any external storage device.
    - Fax transmissions of credit card and electronic payment information occurs only on those fax machines whose access is restricted to only those individuals who must have contact with credit or debit card data to do their jobs. Fax transmissions are strongly discouraged
    - 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 DSS. These standards detail strict encryption protocols.
    - Only secure communication protocols and/or encrypted connections to Elavon and Heartland 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 this information in any form 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 Treasurer's Office.

Departments must use the services of Elavon and Heartland 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 these vendors and wishes to utilize an alternative, it must initiate its request to the Treasurer's Office.

Lehigh University may modify this policy from time to time as required, provided that all modifications are consistent with PCI DSS.

The Treasurer's Office is responsible for initiating and overseeing an annual review of this policy, making appropriate revisions and updates and issuing the revised policy to the 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.

PROCEDURE:

All credit card processing arrangements require the approval of the Treasurer's Office in Finance and Administration. Lehigh University accepts MasterCard, VISA, American Express (AMEX), and Discover. The **MDRP** or his/her designee must follow the steps below in order to implement payment card processing and eCommerce at Lehigh.

1. Contact the Treasurer's Office at 610-758-3180 to determine the appropriate credit card solution (Marketplace or a Payment Card Merchant Account).
2. If applicable, complete the Lehigh University **Payment Card Merchant Agreement**.
3. Submit the Agreement to the Treasurer's Office for review and approval. Allow 2-3 weeks for processing of the request.

If the Agreement is approved, the Treasurer's Office will provide the requesting department any necessary equipment and training.

DEPARTMENTAL RESPONSIBILITIES:

- The department is responsible to process each credit card transaction, receive the proper authorization from Heartland/Elavon for each sale, and to ensure credit card sales are settled daily.
- The department is required to provide to the Bursar's Office a copy of the daily credit card batch along with a deposit transmittal that includes the total of the daily credit card sales and an index and account code. The Bursar's Office is then responsible to post the credit card deposits to the Banner finance system using the information provided.

- Each department is responsible to reply to customer billing disputes and to respond to correspondence from Elavon/Heartland in a timely manner. The department is required to adhere to credit card guidelines set by the processors, which includes specific rules related to internet sales and refunds. The department is required to retain all applicable records, customer authorizations, and copies of receipts in a secure location, and to adhere to the PCI DSS.
- Each department is responsible for reconciling its credit card sales to its Banner index. The Controller's Office reconciles the credit card bank statement and books the monthly processing fees to the department indexes.
- Provide Required Departmental Documentation to the Treasurer's Office, as outlined below.

REQUIRED DEPARTMENTAL DOCUMENTATION:

Payment Card Merchant Agreement –completed annually and submitted with the following attached:

a. **Equipment Inventory Audit Checklist**: Credit card terminals must be periodically inspected to verify make, model and serial numbers. Also, perform a surface inspection to identify attempted tampering or unexpected attachments.

b. **Document Departmental Procedures** : Information detailing methods of payment card acceptance, step-by-step guide how to process payments.

c. **PCI DSS Security Trained Employees List -** A list of every individual in the department with access to payment card information.

d. **Payment Card Security Awareness Acknowledgment** – every individual with access to payment card information must annually complete training and sign the acknowledgement.

e. **Other documentation as needed**

REQUIREMENTS FOR INDIVIDUALS HANDLING OR MANAGING PAYMENT CARD DATA

- Read and understand **Payment Card Policy and Procedures**
- Complete **PCI Security Awareness Training** as necessary
- Sign a **Payment Card Security Awareness Acknowledgment** form