

# DREXEL UNIVERSITY

## Policies and Procedures

Page 1 of 6

### Treasury Department Policy

#### **POLICY: CREDIT CARD MERCHANT POLICY**

#### **POLICY NUMBER:**

**Effective Date: April 13, 2009**

**Responsible Officer: Senior Vice President for Finance, Treasurer & CFO**

#### **I. BACKGROUND:**

The Payment Card Industry (including VISA, Master Card, AMEX, Discover and other major card issuers) has established important and stringent security requirements to protect credit card data. These are called the PCI Data Security Standards or "PCI-DSS". These standards include controls for handling and restricting credit card information, computer and internet security, and reporting of a breach of credit card information.

#### **II. PURPOSE:**

This Policy defines the steps that Payment Card Merchant account holders and eCommerce users at Drexel University must use to access and secure payment card data annually in paper and electronic form. It also establishes responsibility for all steps in the processing of payment card data, self assessment of the merchant account and remediation of processes associated with the transmission, storage or processing of payment card data.

All Drexel payment card merchants must complete an annual self-assessment survey which is submitted to the Treasurer's Office. The Treasurer's office is responsible for submitting the annual Report on Compliance to our acquirer.

This Policy applies to Drexel University and all of its affiliates (collectively, "University" or "Drexel").

Appendix A lists the approved processors and application vendors.

#### **III. DEFINITIONS:**

Acquirer: Bankcard association member that initiates and maintains relationships with merchants that accept payment cards.

Credit Card Information: The full magnetic stripe or the PAN (Primary Account Number) plus any of the following: Cardholder name, Expiration Date or Service Code.

eCommerce: Electronic Commerce consists of the buying and selling of products or services over electronic systems such as the internet and other computer networks.

Merchant Department Responsible Person ("MDRP"): That person designated by a Drexel department as having primary authority and responsibility for eCommerce and payment card transaction processing within that department.

# DREXEL UNIVERSITY

## Policies and Procedures

Page 2 of 6

Payment Card Merchants: A relationship set up by the Treasurer's office between a Drexel University department or other entity and a bank in order to accept payment card transactions.

Self-Assessment: The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

### **POLICY:**

Any Drexel department accepting payment card and/or electronic payments for gifts, goods or services must designate a Merchant Department Responsible Person ("MDRP").

All Merchant Department Responsible Persons must:

1. Ensure that all employees, contractors and agents with access to payment card data within the department acknowledge on an annual basis and in writing (the form is located at the end of this policy) that they have read and understood this Credit Card Merchant Policy. The acknowledgements must be submitted to the Treasurer's Office located in the Main building at 3141 Chestnut Street Room 225 on an annual basis.
2. Ensure that all payment card data collected by the department in the course of performing University business, regardless of how the payment card data are stored (physically or electronically, including but not limited to account numbers, card imprints, and Terminal Identification Number (TIDs)). Data are considered to be secured only if the following criteria are met:
  - Only those with the need-to-know are granted access to payment card and electronic payment data.
  - Email should not be used to transmit payment card or personal payment information. If it should be necessary to transmit payment card information, only the last four digits of the payment card number can be displayed.
  - Payment 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 payment card and electronic payment information can only be on those fax machines whose access is restricted to only 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 Drexel's computers and servers is prohibited. Exceptions will be made only if the processing and storage methods are compliant with Drexel's IRT Information Technology Security Policy, PCI Data Security Standards, and

# DREXEL UNIVERSITY

## Policies and Procedures

Page 3 of 6

this Policy. The Data Security Standards detail strict encryption protocols. Links to these policies and standards are provided at the end of this Policy.

- 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 the payment card (“CVV Code”) is never stored in any form. In the case of American Express, this is a four digit code on the front of the credit card.
- The full contents on any track from the magnetic stripe (on the back of a payment card, in a chip, etc) are never stored in any form.
- All but the first and the last four digits of any payment card account number are always masked if it is necessary to display payment card data.
- All media containing payment card or personal payment data that are no longer needed are destroyed or made unreadable.

No 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 the University may sell, purchase, provide, share, 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 the 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 the department must be coordinated with the Treasurer’s Office.

Departments must use the approved processor 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 approved processor and wishes to utilize an alternative, the MDRP must initiate the request to the IRT and the Treasurer’s Office for a release from the approved processor requirements specified by this policy. Only the Treasurer’s Office and IRT together may authorize the adoption of alternative eCommerce vendors and products.

In the event that the Treasurer’s Office and IRT authorize the use of an alternative eCommerce vendor, then the following must occur:

- The MDRP must provide proof that the alternate eCommerce vendor is certified PCI compliant and ensure that the department and its vendor comply with all relevant provisions of the Drexel University Information Technology Resources Security Policy and the Drexel University Credit Card Merchant Policy.

### **New Merchant Accounts for Credit Card and eCommerce Payments:**

A department that wants to accept credit card payments and/or conduct eCommerce should contact the Treasurer’s Office at 215-895-2803.

### **Responding to a Security Breach**

# DREXEL UNIVERSITY

## Policies and Procedures

Page 4 of 6

In the event of an actual, possible or suspected breach, the department needs to reference and follow the University Data Breach Notification Policy, No. \_\_\_\_\_. In addition, the department must immediately execute each of the additional relevant steps detailed below.

- The MDRP or any individual suspecting a security breach involving eCommerce also must immediately ensure that the following steps, where relevant, are taken to contain and limit the exposure of the breach:
  - a. Prevent any further access to or alteration of the compromised system(s) (i.e., do not log on at all to the machine and/or change passwords; do not log in with ROOT or Administrative authority.)
  - b. Do not switch off the compromised machine; instead, isolate the compromised system(s) from the network by unplugging the network connection cable.
  - c. Preserve logs and electronic evidence.
  - d. Log all actions taken.
- The Treasurer's Office shall alert the acquirer of the suspected breach.

### **RELATED DOCUMENT LINKS:**

Drexel University Data Breach Notification Policy

Drexel University IRT Policy: Acceptable Use  
<http://www.drexel.edu/IRT/policies/acceptableUse.html>

Drexel University IRT Policy: Gramm Leach Bliley Act  
<http://www.drexel.edu/IRT/policies/glba-is-policy-drexel.html>

Drexel University IRT Policy: Security of Enterprise System  
<http://www.drexel.edu/IRT/policies/ses-plan-drexel.html>

Drexel University IRT Policy: Security of Information and Network Systems Plan  
<http://www.drexel.edu/IRT/policies/sins-plan-drexel.html>

PCI Security Standards Council:  
<https://www.pcisecuritystandards.org>

# DREXEL UNIVERSITY

## Policies and Procedures

Page 5 of 6

### **APPENDIX A**

The intent of the Treasurer's office is to minimize the number of vendors that handle credit card data on behalf of Drexel University. The following vendors and their associated processing formats have been approved for use by specific merchant accounts and have PCI compliant language in their contract or in an amendment of their contract.

#### **Payment Processors**

TouchNet

#### **Application Vendors**

Cvent (using Paypal)

Digital Payment Technologies (using Authorized.Net)

EventsPro (using TouchNet T-link)

Harris Connect (using TouchNet T-link)

Simplicity (using TouchNet T-link)

University Tickets (using Authorized.Net)

**DREXEL UNIVERSITY**  
Policies and Procedures

**Payment Card Industry – Data Security Standard (PCI-DSS)  
Policy Attestation**

<b>Department:</b>	
<b>Merchant ID*:</b>	
<b>Director:</b>	

\*The Merchant ID is listed on the side of the credit card machine.

**I have read and acknowledged the following University's security and privacy policies:**

Credit Card Merchant Policy No.  
Data Breach Notification Policy No. [in progress]  
Privacy Policy No. [in progress]

Last Name:

First Name:

Signature:

Date:

Affirmation that you reviewed these policies and procedures satisfies PCI Requirement 12.6.2: "Require employees to acknowledge in writing that they have read and understood the company's security policy and procedure."

Instructions:

1. Update Director with changes.
2. Provide a form for each person who process credit card transaction in your department.
3. Return completed forms to the Treasurer's Office, Main building, Room 225.
4. Contact Peter Keyes at 215-895-2694 or peter.keyes@drexel.edu.