| UNIVERSITY OF Cincinnati | *Policy Title:* **Credit Card Processing** | *Policy Number:* **2.1.27** |
|---|---|---|
| **Category:** Financial | **Effective Date:** 08/01/2011 **Prior Effective Date:** mm/dd/yyyy | **Policy Owner:** Sr. VP for Administration and Finance |
| **Policy applicable for:** Faculty/Staff | **Enabling Acts:** Payment Card Industry Data Security Standards (PCIDSS) | **Responsible Office(s):** Office of the Treasurer |

## Background

The University of Cincinnati is committed to maintaining the highest degree of information security for credit card transactions and data. The purpose of this policy is to establish procedures for processing charges/credits on credit cards to protect against exposure and possible theft of account and personal cardholder information that has been provided to the University of Cincinnati and to comply with the Payment Card Industry Data Security Standards (PCI) requirements for transferring, handling and storage of credit card information.

## Definitions

*Cardholder Data*: Cardholder data is any personally identifiable data associated with a cardholder, such as account number, expiration date, name, address, social security number, card validation code or card identification number.

*Credit Card Merchants*: For purposes of this policy, credit card merchants at the University of Cincinnati are those colleges or organizational units that accept credit cards in payments for products and services.

## Policy

Credit card merchants at the university are required to follow the rules and procedures outlined below to protect customers' credit card data.

The university is phasing out paper processing of credit card information. University credit card merchants will have one year from the effective date of this policy to comply. New applications for credit card processing will be limited to in-person swipe transactions, customer initiated Web-based entry or direct input into credit card device via phone-in order. Existing mail-in processes will be phased out as the Treasurer's Office works with areas currently accepting credit cards by mail. Credit card payments via fax machine are prohibited.

Storage of electronic credit card data on University of Cincinnati computers, servers, laptops or storage media such as CDs or flash drives is prohibited.

Background checks are required for any employee or student involved in credit card processing. The background check must be completed prior to the employee or student

working with credit card data. If the department receives 100% of its credit card payments from customer-initiated payments via the unit website through a compliant gateway such as SkipJack™, the unit is exempt from requiring background checks. If the department has 100% of its credit card payments via transactions where the customer card is present and is swiped using a credit card terminal, this unit is also exempt.

- Credit card data may not be sent through campus mail nor transported by hand from one unit or college to another unit or college.
- Phone order credit card payments must be processed in a secure area. All employees working in the secure area, whether or not they are working specifically with credit card payments, must undergo a background check. A PC (personal computer) used to input credit card payments through a software gateway such as Tickets.com must not have any other applications installed, nor be able to access anything but the Tickets.com credit card application. The unit or college using this PC for credit card payments input must obtain certification regarding the above from their administrative information systems unit and submit this certification to the Treasurer's Office at treasury@uc.edu.
- Merchants may not process credit card payments for other units or colleges.
- The use of wireless networks for credit card processing must be approved in advance by the Treasurer's Office.
- RFPs of any new gateway or credit card processing systems or software and contracts related to these systems must be approved by the Treasurer's Office. Any ancillary software systems connected to credit card processing must be reviewed and approved by the Treasurer's Office prior to purchase or implementation.
- Gateway software connections must be designed so that customers who come to a University of Cincinnati website to make a payment via a credit card input their credit card data on the vendor website and not a university website. There should be a direct link from the UC website to the gateway such as SkipJack™ and any interim pages or steps are prohibited.
- Segmentation of the Card Processing Environment (CPE) will be accomplished through the use of virtual machines (PCs) and virtual networks which will be developed and maintained by UCit.

*Organizational units may institute policies more, but not less, restrictive than this policy 2.1.27) if desired.*

**Related Links:**
Office of the Treasurer
Information Security

**Phone Contacts:**

| | |
|---|---|
| Office of the Treasurer | 556-4510 |
| Information Security | 558-4732 |