# Procedure 6.1401

## Payment Card Industry Data Security Procedure

Payment Card Industry Data Security Standards (PCI-DSS0 Procedure)

In order to comply with Payment Card Industry Data Security Standards (PCI-DSS) as well as good business practices related to the handling of our customers' credit card information:

Purpose

The Payment Card Industry Data Security Standards (PCI DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking and various other security vulnerabilities and threats.

The standards apply to all organizations that store, process or transmit cardholder data. The standards are designed to protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the College.

This procedure is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

General

The College has established relationships with third party entities to process credit card payments. As such the College does not accept (in electronic format), store nor, with the exception of point of sales (POS) terminals, transmit any credit card information.

All departments that collect or have access to credit card information must comply with this PCI DSS Compliance Procedure. These currently include:

- Business Office, accept and transmit credit cards for payment of tuition, fees and transcripts, in person and by phone.
- Book Store, accept and transmit credit card payment for books and course related supplies in person and by phone.
- Continuing Education, accept and transmit credit card information in person and by phone
- Credit card transmission occurs over telephony connections and do not traverse any College network nor reside on any College data processing equipment.

Data Handling

Such data will be treated as confidential.

Data that is not absolutely necessary in order to conduct business will not be retained in any format (e.g., paper or electronic).

We will not accept, request, or retain such data via e-mail or other electronic means.

If we receive credit card data in an email, we will contact the IT Help Desk immediately to have the message removed from our computers and the College email system. We will also notify the sender of the email that the College does not accept credit card information via email and that it should not be attempted again. We will not notify the sender using the Reply function in our email reader as this may inappropriately transmit credit card information.

Captured credit card information, card owner name, credit card number, card-validation code (i.e., the three- or four-digit code) used to validate a card-not-present transaction, personal identification number (PIN) or encrypted PIN block will be deleted immediately upon completion of the financial transaction.

A cross-cut shredder will be used for shredding credit card information

If necessary, credit card information will be placed in a secure shred box for shredding at the earliest opportunity.

Account numbers will be masked if and when displayed (i.e., no more than the first six and last four digits of the credit card numbers).

Physical access to point of sale (POS) terminals used to process credit cards will be restricted.

If such data is shared with any external service provider, we will ensure that:

- A list of providers is maintained;
- A written agreement is executed and retained which defines the provider's responsibility related to the security of this information;
- Any new service provider will be thoroughly vetted by the College Business Office personnel and others as appropriate, before engagement to ensure that the provider can meet these requirements.
- Third party vendors covered by this procedure will be required to conduct their own PCI DSS assessment, and must provide sufficient evidence to the College to verify that the scope of the service providers' PCI DSS assessment covered the services provided to the College and that the relevant PCI DSS requirements were examined and determined to be in place.
- Every service provider's PCI-DSS compliance status is reviewed on an annual basis. Instances of non-compliance are reported to the College Business Office personnel for assistance in determining appropriate follow-up actions.

Roles and Responsibilities

Department personnel assigned to process payment card transactions must be approved by the,

- Director of Accounting
- Director of Campus Operations
- VP Con-Ed
- VP Administrative Services

Departmental personnel approved to process payment card transactions are,

- Bookstore Manager
- Bookstore Assistant
- Administrative Assistant Campus Operations
- Equipment Coordinator
- Accounting Specialist, Cashier
- Accounting Specialist, Accounts Payable
- Records Specialist Con-Ed
- Administrative Assistant Con-Ed

A Credit Card Security Incident Response Plan will be observed and implemented by an Incident Response Team composed of the Departmental Vice President, Director of Accounting and the Vice President of Administrative Services.

The Business Office shall provide appropriate training to staff with security breach response responsibilities.

The Business Office shall provide appropriate training to staff with POS card swipe inspection responsibilities.

The Business Office shall implement a security awareness program for the purpose of making all employees aware of the importance of cardholder data security.

Employees who are approved to use credit card swipe terminals are responsible for examining the terminals for evidence of tampering.

Information Technology shall establish, document and distribute security procedures and related information updates.

**References**

**Legal References:** *Enter legal references here*

**SACSCOC References:** *Enter SACSCOC references here*

**Cross References:** Payment Card Industry Policy

**History**

**Senior Staff Review/Approval Dates:** *05/04/15*

**Board of Trustees Review/Approval Dates:** *Enter date(s) here*

**Implementation Dates:** *Enter date(s) here*