Accepting and Processing Credit Cards

	Policy identification number: **To come...** File: **Business & Finance Policies > Finance and Administration Policies** **Accepting and Processing Credit Cards** Policy Summary **This policy ensures that the College is in compliance with the Payment Card Industry Data Security Standard (PCI DSS), a set of comprehensive requirements for enhancing payment account data security. PCI DSS compliance is mandatory for any organization that collects, processes, or stores credit card information.**

Policy Owner	Approval Date	Effective Date
Vice President for Finance and Administration	**March 18, 2015**	**March 18, 2015**

Search Terms	Scheduled for Review
vpfa, a, c, accepting, processing, credit, cards	**Spring 2020**

I. Applicability

This policy applies to all forms of credit card processing on behalf of the College. Credit card processing includes any payment card transaction (whether credit card, debit card, or other instrument linked to such a card) or other transmission, processing or storage of credit card data regardless of the means by which that transaction occurs. This includes transactions initiated in-person, via the telephone or other telephonic means, in paper form, by U.S. mail or other courier, through a terminal, kiosk, computer system, website, mobile device or any other means.

II. Credit Card Processing

1. Departments that have a charge for services shall have a method for collecting on-campus payments which should include credit card processing. The Controller's Office will assist the department in determining the best method for credit card processing for the campus department's business needs. Campus departments may not negotiate their own contracts with credit card companies, processors, or external services that accept credit card payments on the College's behalf without approval from the Controller's Office. College departments agree to operate in accordance with the contracts the College holds with its service providers and credit card issuers.
2. All credit card payments received must be directed into the College's approved bank account. Departments may not set up their own banking relationships for payment card processing. Any third-party service provider must demonstrate the ability to comply with all College requirements outlined in this policy, most notably PCI DSS and also be able to process the credit card transactions through a Controller-approved Payment Gateway System. A department establishing a contract with a third party is responsible for all associated costs in regard to the payment processing service.
3. Use of imprint machines to process credit card payments is prohibited, as they display the full 16-digit credit card number and expiration date on the customer copy.
4. Wireless credit card processing must be approved by the Controller's Office and can only be done via approved swipe terminals over a cellular connection. Departments cannot process credit card payments via laptops, cell phones, tablets or other similar devices.
5. Employees who handle credit card data agree to not disclose or acquire any information concerning a cardholder's account without the cardholder's consent. Employees will not sell, purchase, provide, disclose or exchange card account information or any other transaction information.

III. Reason for Policy

To mitigate the risk to the College inherent in the acceptance and processing of credit card transactions, to assign the authority and responsibility for such transactions, and to ensure compliance with applicable laws and regulations maintained by the Payment Card Industry Security Standards Council through its Data Security Standard (PCI DSS).

IV. Procedures

1.
    1. The College accepts credit card transactions in face-to-face, mail order, telephone order, secured fax machines or web environments. If accepted by fax, the machine must be located in a secured area with limited access.
    2. Credit card information is not accepted via email or fax-to-email. Departments may not process credit card information transmitted via email or fax-to-email. If an email containing cardholder data is received, it should be deleted immediately

by the recipient, and the sender informed (a) that the transaction was not processed, and (b) of the acceptable channels for the transaction.

3. Credit card information received by mail will be secured at the time it is opened and should be kept in a locked drawer or cabinet until it is processed. The same process shall be used for card information received via fax.
4. Any associated paper or other records or reports containing credit card customer information shall not be maintained unless absolutely necessary as determined by the Controller's Office. If it is absolutely necessary to maintain such information, the paper shall be stored in a locked and secured cabinet or desk. Credit card information will not be stored on any College computer, storage device, or other electronic medium, including imaging, spreadsheets or PDF documents. Access to credit card information and the processing of credit card payments should be limited to those individuals whose job requires such access. Paper records with card numbers should be disposed of through shredding.
5. Departments will transmit receipting information to the Cashier daily (by 2:00 p.m. next day) so that deposits can be recorded into the College's accounting system.

V. Responsibilities

Controller's Office responsibilities: The Controller's Office will provide guidance to departments that accept payments, including the security for credit card transactions and will act as the main point of contact for the merchant services company that processes credit card transactions. The office will provide daily oversight of all credit card transactions and reconcile credit card transactions. The office will assist the Information Technology Department (IT) in responding to PCI self-assessment questionnaires and other surveys.

IT responsibilities: IT will maintain all internal infrastructure related issues for PCI compliance. In the event of unauthorized access or disclosure (breach) of credit card numbers, IT will notify the individuals of the security breach within 14 days, provided notification will not impede a law enforcement investigation. IT will respond to self-assessment PCI compliance surveys from merchant services companies.

Department responsibilities: Departments that accept payment for services shall adopt processes that protect credit card data. Departments are responsible for timely communication with the Controller's Office or IT regarding any credit card inquiries or requests for information, such as for surveys and questionaires regarding credit card processing. Departments who suspect a breach and/or fraud involving credit cards should contact the Controller's Office immediately. Departments must inspect their point-of-sale devices on a regular basis, and should notify the Controller's Office or IT if something appears to be changed, added or different.