

Piedmont Virginia Community College

Section VII – Fiscal Policies & Procedures

VII – 1.3 Credit Card and Payment Card Industry (PCI) Compliance

Effective Date: October 2019

Last Revised: April 2026

Responsible Dept.: Business Office/ Vice President of Finance and Administrative Services

1. Purpose

Accepting credit card payments has become a necessity for increased customer service, especially with the increase in e-commerce. It is essential that the college protect its customers' credit card data.

PCI stands for Payment Card Industry. PCI Data Security Standards are national standards from the Payment Card Security Standards Council and apply to all organizations anywhere in the country that process, transmit and store credit cardholder data.

2. Policy Statement

The college accepts VISA, MasterCard and American Express for payment of tuition and fees for credit and non-credit courses. In addition, credit card payments may be accepted for proctor fees, fines, and performing arts ticket sales. Only approved offices are authorized to take credit card information.

3. Definitions

N/A

4. Applicability

All college staff and faculty must adhere to these procedures and policies. College staff must adhere to procedures to fully safeguard payment card information as required by PCI DSS Standards.

PVCC does not discriminate on the basis of race, color, national origin, sex, disability, or age in its programs and activities. View the full nondiscrimination statement and find contacts at pvcc.edu/nondiscrimination.

5. Responsibilities

N/A

6. Procedures for Implementation

There are two accepted methods for processing transactions: (1) secure website through MYPVCC and (2) card swipe terminal. Other stand-alone systems are not permitted.

Staff members must follow the policies listed below:

- a) Do NOT request or send any credit card information by email
- b) If someone emails cardholder data, you should make them aware that we cannot process the transaction for their own security. Be sure to delete the cardholder's data and the email before responding and suggest an approved payment card processing method.
- c) Never record data in any electronic format such as excel or any databases.
- d) Do not request, record or store any of the magnetic striped data, the credit card confirmation code, or cardholder account numbers with expiration dates. The confirmation code is sometimes referred to as the "CVV2" code that appears on the back of the credit card.
- e) Do not direct a payer to a specific college owned computer or offer to enter payment card data into a hosted website on their behalf.
- f) Credit card information received by mail or fax must be shredded once the transaction has been posted. Due diligence must be taken to protect written card information at all times. Do not leave card information on open desks or locations that are accessible to the public.
- g) There may be times when credit card information is taken by phone. Verify the cardholder's name, phone number, credit card number, and expiration. Any written information must be processed as quickly as possible, and all written information must be shredded upon approval of the credit card transaction.
- h) Credit card transactions in excess of amounts due are not permitted.
- i) The college does not accept payments through Pay Pal.
- j) Students should be encouraged to make credit card payments through MyPVCC as this information is PCI protected.
- k) Credit card information must not be stored or filed. A copy of the swipe receipt, which does not include sensitive information, may be filed with the student receipt.
- l) Credit card information should not be taken through voicemail. Should a person leave

credit card information on voicemail, delete at once and notify the individual that you cannot process their payment and suggest an approved payment process.

7. Sanctions for Violation of Policy

N/A

8. Other General Information

N/A