PIEDMONT VIRGINIA COMMUNITY COLLEGE

VII. FISCAL POLICIES AND PROCEDURES

VII-1.3 CREDIT CARDS AND PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY

Policy #: VII-1.3
Effective: October 2019
Responsible Dept.: Business Office

I. INTRODUCTION

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 customer's credit card data. College staff must adhere to procedures to fully safeguard payment card information as required by PCI DSS Standards. 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.

II. POLICY

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. 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:

1. Do NOT request or send any credit card information by email
2. 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 data and the email before responding and suggest an approved payment card processing method.
3. Never record data in any electronic format such as excel or any databases.
4. Do not request, record or store any of the magnetic stripe 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.
5. 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.
6. 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.
7. There may be times that credit card information is taken by phone. Verify the cardholders name, phone number, credit card number and expiration. Any information written down must be processed as quickly as possible and all written information must be shredded upon approval of the credit card transaction.
8. Credit card transactions in excess of amounts due are not permitted.

9. The college does not accept payments through Pay Pal.
10. Students should be encouraged to make credit card payments through MyPVCC as this information is PCI protected.
11. 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.
12. 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 can not process their payment and suggest an approved payment process.

If a security breach involving cardholder information is detected immediately notify the business manager and the Information Security Officer.

All employees who work with credit card data will be required to sign a Payment Card Confidentiality Agreement.

All employees are required to complete data security training once a year.

Annually, the college will contact the third party vendors on campus to obtain their PCI DSS compliance status.