SOUTHERN WEST VIRGINIA COMMUNITY AND TECHNICAL COLLEGE
BOARD OF GOVERNORS
SCP-5XXX

SUBJECT: PCI Compliance and Merchant Services

REFERENCE: WV State Code 12-3A-6; WV State Treasurer's Office Credit Card Handling Handbook; Payment Card Industry Data Security Standards (PCI-DSS)

ORIGINATION: February 9, 2024

EFFECTIVE:

REVIEWED:

SECTION 1. PURPOSE

1.1 The purpose of this Policy is to establish the compliance requirements for Southern West Virginia Community and Technical College to process payment cards consistent with Payment Card Industry Data Security Standards (PCI-DSS), WV State Code as administered through the WV Treasurer's Office, and applicable federal and state laws and regulations.

SECTION 2. SCOPE AND APPLICABILITY

2.1 This policy applies to all college departments, employees, vendors, consultants, and other authorized persons associated with the College to utilize the College's Merchant Services.

SECTION 3. DEFINITIONS

3.1 "Payment Cards" can be credit, debit, charge, and prepaid cards; a form of payment electronically linked to an account or accounts belonging to the cardholder. For the College's Merchant Services program, payment cards are credit and debit cards.

3.2 "Cardholder Data" means personally identifiable information associated with a credit/debit card user, including the account number, expiration date, name, address, or Social Security number.

3.3 "Merchant Services" means the process of conducting payment transactions over electronic means. Although primarily conducted via the Internet, this can also include automated phone banks, touchscreen kiosks, and ATMs. Transactions have payment cards or electronic funds transfers via Automated Clearing House (ACH).

3.4 "Merchant Bank," also known as an Acquiring Bank, is the bank or financial institution that processes payment card transactions for a merchant.

3.5 "College Merchant" is a College division, department, or other applicable unit that processes payment card payments using a POS device, a 3rd party system, or an eCommerce website.

3.6 "Payment Card Industry Council" is the governing body overseeing how payment card transactions are processed.

3.7 "Payment Card Industry Data Security Standards (PCI-DSS) means a consolidated standard from the major payment card issuers detailing merchant requirements when accepting credit/debit cards, including Visa, MasterCard, American Express, Discover, and JCG. The requirements include network security (physical/logical) and monitoring components.

3.8 "Payment Gateways" are the approved Merchant Services solutions provided by the West Virginia State Treasurer's Office to collect payment card payments over the Internet.

3.9 "Personal Data" means information or data collected that can identify an individual directly or indirectly.

3.10 "Point to Point Encryption" means the information is encrypted instantly upon initial swipe/dip and then securely transferred to the payment processor before it is decrypted and processed.

SECTION 4. POLICY

4.1 The College is responsible for processing and reconciling payments using payment cards consistent with PCI-DSS and WV State Code, regardless of whether payment is received in person, over the phone, or using a College eCommerce website.

4.2 The College's Information Technology (IT) network is deemed to be out of scope for supporting Point of Sale (POS) transactions that do not encrypt the transaction. Only Payment Card Industry (PCI) Council-approved POS devices that use Point-to-Point Encryption technology (P2PE) may be connected to the College's IT network for College Merchants to process payment card transactions. The use of unapproved POS devices is strictly prohibited.

4.3 All College Merchants utilizing the Internet to accept payment card payments must utilize the West Virginia State Treasurer's Office (WVSTO) approved Payment Gateways. Use of unapproved Payment Gateways is prohibited.

4.4 All POS and Payment Gateways must be associated with an approved OASIS account. Use of any other type of bank account is prohibited.

4.5 To ensure compliance, a College Merchant must have a legitimate business need to process payments using payment cards to support their administrative, outreach, or academic mission. A legitimate business need must be identified for the designation of College Merchant to be granted.

4.6 Use of email to accept payment card payments is strictly prohibited.

SECTION 5. BACKGROUND AND EXCLUSIONS

5.1 None

SECTION 6. GENERAL PROVISIONS

6.1 Any employee who violates this Policy will be subject to appropriate disciplinary action.

6.2 Any student who violates this Policy will be subject to the appropriate disciplinary action in accordance with the Student Code of Conduct.

6.3 Any individual affiliated with the College who violates this Policy will be subject to appropriate corrective action, including, but not limited to, termination of the individual's relationship with the college.

6.4 College Merchants who do not comply with this Policy may be subject to appropriate penalties, including revocation of status as College Merchant. In the event of a data breach due to non-compliance, College Merchants may be subject, but not limited to, the following:

6.4.1 Fines imposed by a bank and/or payment brand

6.4.2 Cost to notify cardholders of a data breach

6.4.3 Payment Card replacement and remediation services for impacted cardholders

6.4.4 Repayment of fraudulent charges resulting from a data breach

6.4.5 Onsite forensics audit by a PCI-Qualified Data Security Company

6.4.6 Merchant certification by a PCI-Qualified Date Security Company

6.4.7 Associated legal fees

6.5 The College's Chief Finance Officer, supported by the Bursar, Controller, and Chief Information Officer, will coordinate with appropriate College entities on implementing and enforcing this policy.

6.6 Responsibility for interpreting this Policy rests with the Chief Finance Officer.

SECTION 7. RESPONSIBILITIES

7.1 The Business Services Unit is responsible for leading and overseeing the College's Merchant Services Program, which includes the following activities:

7.1.1 Working with the WVSTO to ensure that the College's Merchant Services program is in compliance with PCI-DSS, WV State Code, and other federal and state laws and regulations;

7.1.2 Designating the College Merchants who have a legitimate business need to accept payment card payments on behalf of the College:

7.1.3 Maintaining an inventory of all POS devices, eCommerce websites, and Payment Gateways. Maintaining a list of College Merchants with their associated Merchant ID numbers and completed SAQs, and maintaining a list of vendors' PCI Attestation of Compliance in use at the College.

7.1.4 Ensuring that the College Merchant provides and completes annual PCI security and awareness training.

7.1.5 Collaborating with Information Technology (IT) on developing policies and procedures to establish a governance framework for the College Merchant Services Program.

7.1.6 Collaborating with IT on completing and submitting the PCI Self-Assessment Questionnaire (SAQ) for submission to the WVSTO Merchant Bank.

7.2 Information Technology will support the College Merchant Services Program, which includes the following activities:

7.2.1 Conducting security risk assessments of College Merchants to ensure that their processing of payment card payments does not introduce an information security risk to the College's IT environment and to ensure that their payment card payment processing complies with PCI Standards.

7.2.2 Collaborating with the Business Services Unit on developing policies and procedures to establish a governance framework for the College Merchant Services Program.

7.2.3 Collaborating with the Business Services Unit on the completion and submission of PCI Self-Assessment Questionnaires (SAQs) for submission to the WVSTO's Merchant Bank.

7.2.4 Provide IT technical support to the College's Merchant Services program.

7.3 College Merchants are responsible for the following:

7.3.1 Designating an individual within the department who has primary authority and responsibility for the payment card transaction processing by that College Merchant.

7.3.2 Ensuring that daily settlements for payment card transactions are entered into the College financial system.

7.3.3 Ensuring all staff with duties to accept or process payments complete annual security awareness training (e.g., PCI-DSS, identity theft detection) provided by the College.

7.3.4 Distributing the tasks of processing payment, balancing daily transactions, and balancing books between at least two different people.

7.3.6 Using College-provided, validated POS to collect Cardholder Data over the phone or in person.

7.3.7 Using WV State Treasurers' Office approved Payment Gateway to facilitate payment for products, goods, and services were available on the College websites.

7.3.8 Ensuring that goods and services offered for sale on College websites are reflected accurately.

7.3.9 Complying with College policies, procedures, and standards, including but not limited to the Security of Information Technology Policy and the Information Technology Acceptable Usage Policy.

7.3.10 Reporting known or suspected Security Incidents to Information Technology.

Section 8. CANCELLATION

8.1 None

Section 9. REVIEW STATEMENT

9.1 This policy shall be reviewed on a regular basis with a time frame for review to be determined by the President or the President's designee. Upon such a review, the President or the President's designee may recommend to the Board that the policy be amended or repealed.

Section 10. SIGNATURES

_____

Board of Governors Chair **Date**

_____

President **Date**

Attachments: None

Distribution: Board of Governors (12 members)
www.southernwv.edu

Revision Notes: February 9, 2024 – Policy originated.