Policy 5.1.1
Merchant Services Policy

Category: Finance
Title: Merchant Services Policy
Responsible Unit: Revenue Services
Effective: 6.11.21 (Digitally Signed by Anjali Halabe)
Revision History: Replaces Electronic Commerce Services Policy originally effective October 31, 2001
Review Date: 2023

POLICY 5.1.1
MERCHANT SERVICES POLICY

1. PURPOSE & SCOPE:

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

1.2 This Policy applies to all University departments, employees, vendors, consultants, and other authorized persons associated with the University to utilize the University's Merchant Services (University Merchants).

2. UNIVERSITY MERCHANT SERVICES FRAMEWORK:

2.1 The University is responsible for the processing and reconciliation of 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 University eCommerce website.

2.2 The University'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 University's IT network for use by University Merchants to process payment card transactions. Use of unapproved POS devices is strictly prohibited.

2.3 All University Merchants utilizing the Internet to accept payment card payments must utilize the West Virginia State Treasurer's Office (WV STO) approved Internet Payment

Gateways. A list of approved payment gateways can be found in the Merchant Services procedure. Use of unapproved Internet Payment Gateways is prohibited.

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

2.5 To ensure compliance, a University Merchant must have a legitimate business need to process payments using payment cards in support of their administrative, research, outreach, or academic missions.. If a legitimate business need cannot be identified, the designation of University Merchant cannot be granted.

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

---

3. UNIVERSITY MERCHANT SERVICES PROGRAM RESPONSIBILITIES:

3.1 The Division of Finance is responsible for leading and overseeing the University's Merchant Services Program, which includes the following activities:

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

3.1.2 Designating the University Merchants who have a legitimate business need to accept payment card payments on behalf of the University;

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

3.1.4 Ensuring that University Merchant are provided and complete annual PCI security and awareness training;

3.1.5 Collaborating with Information Technology Services (ITS) on developing policies and procedures to establish a governance framework for the University Merchant Services Program;

3.1.6 Collaborating with ITS on the completion and submission of PCI Self Assessment Questionnaires (SAQs) for submission to the WV STO's Merchant Bank.

3.2 Information Technology Services will support the University Merchant Services Program, which includes the following activities:

3.2.1 Conducting security risk assessments of University Merchants to ensure that their processing of payment card payments does not introduce an information security risk to the University's IT environment and to ensure that their payment card payment processing is in compliance with PCI standards;

3.2.2 Collaborating with the Division of Finance on developing policies and procedures to establish a governance framework for the University Merchant Services Program;

3.2.3 Collaborating with the Division of Finance on the completion and submission of PCI Self Assessment Questionnaires (SAQs) for submission to the WV STO's Merchant Bank and;

3.2.4 Provide IT technical support to the University's Merchant Services program.

---

4. UNIVERSITY MERCHANT RESPONSIBILITIES:

4.1 University Merchant are responsible for the following:

4.1.1 Designating an individual within the department who has primary authority and responsibility for the payment card transaction processing by that University Merchant;

4.1.2 Ensuring that daily settlements for payment card transactions are entered into the University's financial system.

4.1.3 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 University;

4.1.4 Distributing the tasks of processing payments, balancing daily transactions, and balancing books between at least two different people;

4.1.5 Ensuring that all employees, including students, who will process payments have a background check conducted as part of on-boarding hiring process;

4.1.6 Using University-provided, validated POS to collect Cardholder Data over the phone or in person;

4.1.7 Using STO-approved Payment Gateways to facilitate payment for products, goods, and services available on University websites;

4.1.8 Ensuring that goods and services offered for sale on University websites are reflected accurately;

4.1.9 Complying with University policies, procedures, and standards, including but not limited to the Sensitive Data Protection Policy, Information Privacy Policy, and Computer Security Incident Response Policy.

4.1.10 Reporting known or suspected Security Incidents to Information Technology Services pursuant to the Computer Security Incident Response Policy.

---

5. DEFINITIONS:

5.1 "Payment Cards" can be credit cards, debit cards, charge cards and prepaid cards. It's a form of payment that's electronically linked to an accont or accounts belonging to the card holder. For the University's Merchants Services program payment cards are credit and debit cards.

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

5.3 "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, touch screen kiosks, and ATMs. Transactions include payment cards or electronic transfer of funds via Automated Clearing House.

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

5.5 "University Merchant" is a University regional campus, college, division or other applicable unit that processes payment card payments using a POS device, a 3rd party system or through an eCommerce website.

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

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

5.8 "Payment Gateways" are the approved Merchant Services solutions provided by the STO to collect payment card payments over the Internet.

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

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

---

6. ENFORCEMENT AND INTERPRETATION:

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 appropriate disciplinary action in accordance with the Student Code of Conduct.

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

6.4 University Merchants who do not comply with this Policy may be subject to appropriate penalities including revocation of status as University Merchant. In the event of a data breach due to non-compliance, University 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 Costs 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 Data Security Company; and,

6.4.7 Associated legal fees.

6.5 The University's Vice President and Chief Financial Officer, supported by the Associate and Assistant VPs for Finance and the Chief Information Security Officer, will coordinate with appropriate University entities on the implementation and enforcement of this Policy.

6.6 Responsibility for interpretation of this Policy rests with the Chief Financial Officer.

---

7. AUTHORITY & REFERENCES:

7.1 West Virginia State Code WV § 12-3A-6

Category: Finance
Title: Merchant Services Policy
Responsible Unit: Revenue Services
Effective: 6.11.21 (Digitally Signed by Anjali Halabe)
Revision History: Replaces Electronic Commerce Services Policy originally effective October 31, 2001
Review Date: 2023

7.2 BOG Governnce Rule 5.1 Authorizations and Delegations of Authority for Financial and Administrative Matters

7.3 All other University policies are also applicable to the electronic environment. Relevant institutional policies include, but are not limited to:

7.3.1 Information Privacy Policy

7.3.2 Identity Theft Detection and Prevention Policy

7.3.3 Sensitive Data Policy

7.3.4 Sensitive Data Protection Standard

7.3.5 Faculty Handbook

7.3.6 Code of Student Rights and Responsibilities

Signature: Electronically Approved Date: 6.10.21
Anjali Halabe
Sr. Associate VP for Finance