COLUMBUS STATE UNIVERSITY

Policy Name:	Payment Card Industry Data Security Standard (PCI-DSS) Compliance Policy
Policy Owner:	Chief Operating Officer
Responsible University Office:	Office of Business and Finance
Approval Date:	January 21, 2025
Effective Date:	January 21, 2025
Related Policies:	N/A

I. POLICY STATEMENT

This policy establishes the requirements for the protection and security of cardholder data at Columbus State University (CSU). The university is committed to maintaining compliance with the Payment Card Industry Data Security Standard (PCI DSS) to protect cardholder information and ensure the security of all transactions involving payment card data. As part of Columbus State University's commitment to security, the university does not store or hold credit card data in any form.

II. PURPOSE AND SCOPE

The purpose of this policy is to outline the requirements and responsibilities for protecting cardholder data and to ensure that all university departments and personnel handling payment card transactions comply with PCI DSS requirements.

This policy applies to all faculty, staff, contractors, and any other entities involved in processing, transmitting, or storing cardholder data on behalf of Columbus State University. It covers all payment channels including, but not limited to, online transactions, point-of-sale (POS) systems, and mail/telephone orders.

III. DEFINITIONS

- **Cardholder Data**: Any personally identifiable information associated with a cardholder, including Primary Account Number (PAN), cardholder name, expiration date, and service code.
- **PCI DSS**: A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

IV. POLICY

Columbus State University commits to adhering to the following key PCI DSS requirements to protect cardholder data:

1. **Build and Maintain a Secure Network and Systems**: Implement robust firewall and security configurations to protect cardholder data.
2. **Protect Cardholder Data**: Ensure that all cardholder data is securely stored and encrypted during transmission.
3. **Maintain a Vulnerability Management Program**: Regularly update anti-virus software and develop secure systems and applications.
4. **Implement Strong Access Control Measures**: Restrict access to cardholder data based on business needs and ensure proper identification and authentication.
5. **Regularly Monitor and Test Networks**: Continuously track access to network resources and cardholder data, and regularly test security systems.
6. **Maintain an Information Security Policy**: Develop and maintain an information security policy that addresses all personnel involved in cardholder data handling.
7. **Training**: Provide comprehensive training on PCI DSS compliance and data protection to all relevant personnel, ensuring they understand their responsibilities.

By adhering to these requirements, Columbus State University aims to protect cardholder data, ensure compliance with PCI DSS standards, and maintain the integrity of payment card transactions.

V. PROCEDURES

It is the policy of the University to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Finance Department. All card handling activities and related technologies must comply with the PCI DSS in its entirety. No activity may be conducted, nor any technology employed that might obstruct compliance with any portion of the PCI DSS. ***Columbus State University shall comply with the current version of the PCI DSS.***

1. Any authorized unit of the University permitted to accept credit/debit cards as a form of payment will be required to comply with the guidelines and procedures issued by the Finance Department and the Office of Student Accounts.
2. If a Unit or Department is considering using a 3rd party vendor or 3rd party software application to accept payments, the department must complete the 3rd party vendor application through IT Security Approval must be granted from the PCI Steering Committee and IT security prior to signing any agreements or purchasing such software.
3. All in-person credit card processing must be P2PE compliant. Departments are not permitted to set up their own merchant accounts or purchase their own credit card terminals.
4. All e-commerce credit card processing must be compliant with PCI/DSS SAQ A-EP. When reviewing vendor proposals, departments should ensure that the vendor is capable of annually proving compliance with PCI/DSS through an Attestation of

Compliance (AOC)

5. The approved vendor for Columbus State University is TouchNet. If a department wishes to accept e-commerce payments and does not currently utilize TouchNet, they will be directed to the Office of Student Accounts for assistance with the setup of a TouchNet Marketplace store.
6. All processing equipment (terminals, registers, computers, etc.) must be approved by the PCI Steering Committee before purchase.
7. CSU contracts shall require such vendors, contractors, and business partners to be compliant with the PCI DSS.
8. The university will not become a service provider for any external vendor.
9. Exceptions to this policy are limited and will require a business plan and justification. This request must be submitted and approved by the PCI Steering Committee in advance of initiation of new business process and equipment /system purchase.

This policy is reviewed annually and updated as necessary to ensure ongoing compliance with PCI DSS requirements and CSU business objectives.

APPROVED: Signed by: Stuart Rayfield 9021BECE669B417... _____

Dr. Stuart Rayfield, President

Date: 1/22/2025 | 8:50 AM EST _____