POLICY: 6Hx28:7B-05

Responsible Executive: Chief Information Officer

Policy Contacts: Managing Director, CISO

Specific Authority: 1001.64, F.S.

Law Implemented: 1001.64, F.S.

Effective Date: 09-11-2025

Date of Last Policy Review: 09-11-2025

Payment Card Processing Standards

Policy Statement:

I. Valencia College ("College") is committed to security, confidentiality, integrity, availability, and accountability with regard to the personal and sensitive information it collects, creates, uses, and maintains. This policy defines, documents, and supports the implementation and maintenance of the College's payment card processing standards to the extent that the College accepts payment cards in-person, through telephone, and through online payments. The College shall take reasonable measures to protect and secure data containing such information in accordance with applicable laws, rules, regulations, and College policies.

II. The College shall establish a set of roles and responsibilities to implement, oversee, and maintain compliance with the applicable requirements of the Payment Card Industry Data Security Standard (PCI DSS).

III. The College shall require any of its departments or offices that accept payment cards for transactions of any goods or services to designate an employee(s) to manage their compliance with the PCI DSS and any other related requirements set forth by the College through policy, procedures, or other guiding documents.

IV. Third-party service providers contracted by the College to perform payment processing services must maintain compliance with PCI DSS and provide the College with an Attestation of Compliance, upon request. The College shall include this requirement on any contract or agreement established with an authorized service provider.

V. The College President or designee(s) may adopt procedures to implement this policy.

Policy History: Adopted 9-11-25

Related Documents/Policies:

College Policy 6Hx28: 7A-01 Information Security Program

College Policy 6Hx28: 3E-08 Disciplinary Action

College Policy 6Hx28: 7B-04 Financial Information Security Program

College Policy 6Hx28: 8-03 Student Code of Conduct

Procedures:

I. Definitions:

1. Account Data: Cardholder data and/or sensitive authentication data.

2. Cardholder Data ("CHD"): Sensitive information associated with a payment card, which consists of, at a minimum, the full unique primary account number (PAN).

3. Sensitive Authentication Data ("SAD"): Security-related information used to authenticate a cardholder and/or authorize a payment card transaction (e.g., card verification code or PIN).

4. Card Data Environment ("CDE"):

    1. System components, people, and processes that store, process, or transmit CHD and/or SAD; and

    2. System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD

5. System Components: Any network devices, servers, computing devices, virtual components, or software included in or connected to the CDE, or that could impact the security of cardholder data and/or sensitive authentication data.

6. Merchant Manager: The designated College employee in each division responsible for PCI Compliance of a merchant account. This includes but is not limited to PCI DSS, PCI training, and maintaining documents for PCI audit.

7. Information Security Program Administrator: The designated College employee responsible for the College's information security program.

8. Attestation of Compliance: A document that formally declares a business' compliance

with a specific standard, such as the PCI DSS, to maintain security best practices for protecting sensitive data.

II. College Roles and Responsibilities for Payment Card Processing

A. The Merchant Manager is assigned as the point of contact for the service or operation that provides a good or service and accepts payment cards for such service(s). The Merchant Manager is responsible for:

1. Maintaining compliance with any and all relevant PCI standards for their operation and will maintain vendor relationships with any and all third-party service providers or payment processors used in conjunction with payments made on their goods and services. This includes obtaining *Attestation of Compliance* documents from these providers upon request.

2. Completing any audits or assessments for the merchant accounts they manage required by the Merchant Bank.

3. Ensuring that the employees within their supervision or division that interact with account or cardholder data, as appropriate, complete all required information security and PCI compliance training offered by the College.

B. The Information Security program Administrator is the main point of contact for any potential security event involving account data and is responsible for:

1. Maintaining this policy and establishing procedures used by Merchant Managers and their staff, as well as any authorized third-party service provider or payment processor that conducts any payment transactions on behalf the College.

2. Reviewing all agreements and contracts with any service provider that collects, stores, or transmits cardholder data for the College and validating that the solutions procured meet PCI security standards.

3. Assessing or overseeing third-party service providers that are hired to assess the controls in place to safeguard account data.

III. Guidelines Governing the Use of Payment Cards

A. The College will obtain a copy of and review the PCI DSS Attestation of Compliance form(s) for all third-party service providers and confirmed that these third-party service providers are PCI DSS compliance for the services used by the College.

B. The College will not electronically store, process, or transmit any account data on College systems or premises and will rely on a PCI DSS compliant third-party service providers and/or payment processors to manage these functions. The following are applicable to third-party service providers and/or payment processors:

1. Any cardholder name, primary account number, service code, and/or expiration date, or otherwise present within the CDE must be protected in accordance with the PCI DSS requirements.

2. Payment processing for all card-present transactions must be completed via a validated PCI-listed Point-to-Point Encryption (P2PE) solution. All controls provided by the P2PE solution provider must be implemented.

3. Only payment terminals from validated PCI-listed P2PE solutions may be used to store, process, or transmit account data for transactions conducted on any College property.

4. For all e-commerce transactions, all elements of the payment page(s) or form(s) delivered to the customer's browser must originate only and directly from the PCI DSS compliance third-party service providers or payment processor.

C. Any account data the merchant might retain is on paper and these documents are not received electronically. Examples of allowed documents are receipts and printed reports. The College will not request or send this data in any digital form.

IV. Reporting Violations

A. Reports of alleged policy and/or procedure violation(s) should be reported to the Office of Information Technology (OIT) at 407-582-5555 or OITServiceDesk@valenciacollege.edu for initial evaluation. Based on the nature and severity of the allegations, OIT will partner with Organizational Development and Human Resources if a College inquiry, investigation, or further assistance is needed.

B. If it is determined that a violation has occurred and depending on the nature and severity of the offense, violators of this policy and/or its implementing procedures may be subject to additional and appropriate College action, including but not limited to, College disciplinary action; denial of College technology access and/or College property; and/or criminal prosecution under applicable laws, rules, and regulations. For more information, see College Policies 6Hx28: 3E-08 Disciplinary Action.

Procedure History: Adopted 9-11-25

Related Documents/Procedures:

Date of Last Procedure Review: 09-11-2025