Procedure III.3001.K.a, Payment Card Industry Data Security Standard (PCI DSS)

Associated Policy
Policy III.3001.K, Payment Card Industry Data Security Standard (PCI DSS)

Purpose
This procedure establishes the operational processes and lifecycle activities required to implement and maintain PCI DSS compliance across the College.

The procedure defines how the College governs payment card processing activities, including the approval and management of payment systems, coordination of third-party service providers, and maintenance of required documentation supporting PCI DSS compliance for College business.

It outlines the processes for identifying and managing PCI DSS scope, validating compliance of vendors and systems, and ensuring that payment card environments are maintained in accordance with applicable security standards.

The procedure also defines requirements for recurring compliance activities, including vendor attestation validation, completion of applicable self-assessment requirements, and periodic review of payment processing environments to ensure continued compliance.

Additionally, the procedure establishes expectations for training, communication, and awareness for employees involved in payment processing, as well as coordination between the Business Office and the Office of Cybersecurity for monitoring, risk management, and incident response related to payment card activities.

This procedure supports the ongoing management, monitoring, and continuous improvement of the College's PCI DSS compliance program.

Procedures

I. Payment Card Environment Identification and Risk Assessment

1. The Student Financial Services Department (or designee) will coordinate a college-wide review of payment card processing activities at intervals defined by the College's PCI DSS compliance calendar to identify payment systems, cardholder data flows, third-party service providers, and associated risks.
2. Each division, campus, and department accepting payment cards will provide information using College-approved templates or systems to document:
    - Payment methods and processing locations
    - Systems and devices used to accept payments
    - Third-party vendors supporting payment processing
    - Points where cardholder data is transmitted or handled
3. A risk assessment will be conducted in conjunction with the review to identify threats, vulnerabilities, and potential impacts to the confidentiality and security of cardholder data.

4. The Student Financial Services Department will consolidate results, validate findings with leadership and the Office of Cybersecurity, and identify institution-level PCI DSS scope, risk exposure, and compliance priorities.
5. Results will be reviewed with the Strategic Leadership Team (SLT) or its designee and updated at least annually, following significant system changes, or after identified security events.

II. Development and Maintenance of Payment Card Processes and Controls

1. Finance leaders responsible for payment processing will ensure that departmental payment card processes are developed, approved, and maintained in alignment with San Jacinto College policy and PCI DSS requirements.
2. Departmental processes will be developed using College-approved standards and will, at a minimum, address:
    - Approved payment methods and systems
    - Roles and responsibilities for staff handling payments
    - Secure handling of cardholder data
    - Vendor involvement and third-party processing
    - Reconciliation and documentation requirements
3. Payment card systems and processes will be submitted to the Student Financial Services Department for review, alignment with institutional requirements, and inclusion in the College's PCI DSS inventory.
4. Payment processes and system usage will be reviewed at least annually and updated when significant changes occur to operations, technology, vendors, or regulatory requirements.
5. Department leaders will ensure staff involved in payment processing are aware of approved processes, understand their responsibilities, and know how to respond to potential security concerns.

III. Approval, Implementation, and Decommissioning of Payment Systems

1. The Student Financial Services Department will coordinate the approval and implementation of all payment card systems to ensure alignment with PCI DSS requirements and institutional standards.
2. Departments requesting new or modified payment systems must submit requests through college-approved processes prior to implementation.
3. Upon approval:
    - The Student Financial Services Department will document the system within the PCI DSS inventory
    - Departments will implement approved systems and processes

- The Office of Cybersecurity will provide advisory input as needed regarding system security and PCI DSS scope

4. Payment systems will be reviewed periodically to ensure continued compliance and alignment with San Jacinto College standards.
5. Systems that are no longer required, no longer compliant, or present elevated risk will be decommissioned in coordination with the Student Financial Services Department and relevant stakeholders.
6. Departments will transition from retired systems to approved alternatives and ensure that all associated access, documentation, and records are appropriately updated.

IV. Compliance Activities, Monitoring, and Incident Response

1. The Student Financial Services Department will coordinate annual PCI DSS compliance activities in alignment with the College's audit and compliance calendar.
2. Annual compliance activities will include:
    - Validation of third-party service provider compliance
    - Completion of applicable PCI DSS self-assessment requirements
    - Review of payment systems and processing environments
3. The Office of Cybersecurity will monitor the Payment Card Environment and perform security activities, including:
    - Log monitoring and review
    - Internal vulnerability scanning
    - External vulnerability scanning by an approved vendor
    - Periodic penetration testing
4. Suspected security incidents involving payment card data will be reported to the Student Financial Services Department and the Office of Cybersecurity in accordance with the College's incident response processes.
5. The Student Financial Services Department and the Office of Cybersecurity will coordinate response efforts, documentation, and communication related to PCI DSS related incidents.

V. Training, Awareness, and Continuous Improvement

1. The Student Financial Services Department in collaboration with the Comptroller's Office and Information Technology Services will coordinate PCI DSS training and awareness activities for employees involved in payment card processing.
2. Department leaders will ensure staff complete required training and adhere to approved processes for handling cardholder data.
3. Training and awareness efforts will reinforce:

- Secure handling of cardholder data
- Use of approved payment systems
- Reporting of potential security concerns

4. After compliance reviews, assessments, or incidents, the Student Financial Services Department will evaluate outcomes to identify opportunities for improvement.
5. Identified improvements will be documented, assigned, and incorporated into updated processes and controls.
6. PCI DSS awareness will be incorporated into onboarding or role-based training for employees with payment processing responsibilities.

Definitions

- Payment Card Industry Data Security Standard (PCI DSS): Global set of requirements to protect cardholder data and reduce fraud.
- Cardholder Data (CHD): Includes PAN, cardholder name, expiration date, and service code.
- Primary Account Numbers (PAN): The unique identifier for a cardholder's account.
- Sensitive Authentication Data (SAD): Includes magnetic stripe data, CVV, or PINs, and must never be stored post-authorization.
- PCI DSS Compliant System: Meets all PCI DSS controls, including encryption, restricted access, and regular audits.
- Third-Party Service Provider: Vendor handling payment card data on behalf of the College.

Date of SLT Approval	May 12, 2026
Effective Date	August 11, 2026
Associated Policy	Policy III.3001.K, Payment Card Industry Data Security Standard (PCI DSS)
Primary Owner of Policy Associated with the Procedure	Vice Chancellor, Fiscal Affairs
Secondary Owner of Policy Associated with the Procedure	Associate Vice Chancellor, Finance