THE TRUSTEES OF TRINITY COLLEGE
POLICY ON PAYMENT CARD ACCEPTANCE

Trinity College Policy No. 9.4

Policy Statement

Trinity College accepts payment cards (e.g., credit cards and debit cards) for the convenient payment of goods and services and receipt of donations. The use of payment cards on campus must comply with this policy as established by Accounting Services as well as the Payment Card Industry Data Security Standard (PCI DSS) requirements, which are intended to limit exposure and/or theft of personal cardholder information. This policy establishes the requirements for accepting and processing payment cards and the protection of cardholder data.

This policy applies to all College departments, units, employees, faculty, students, student clubs and organizations, affiliates, contractors, guests, consultants, temporary employees, and any other users who accept donations or sell goods, services, or information, and who accept payment cards as a form of payment on behalf of the College.

All computers and electronic devices (collectively called technology resources) used for processing payment card data are subject to this policy and must meet PCI DSS requirements. This includes workstations used to enter payment card information and computers or payment card swipe devices through which payment card information may be transmitted.

Definitions

Cardholder Data Environment (CDE)
The people, operations, and technology that store, process, and/or transmit cardholder data (CHD) or sensitive authentication data. A CDE also includes any component that directly connects, supports, or may otherwise affect the security of this environment.

Merchant(s)
All persons, departments, units, entities, and third-party service providers acting on behalf of the College that accept payment cards bearing the logos of any of the five members of the Payment Card Industry Security Standards Council (PCI SSC; includes American Express, Discover, JCB, MasterCard, and Visa) as a method of payment for goods and/or services.

Merchant Account
A unique account set up with Trinity College's bank that provides a department, unit, or entity with the ability to process and settle payment card transactions for goods, services, or donations.

Payment Card
Credit cards, debit cards, and some gift/stored-value cards that bear the logo of a card association brand, including but not limited to American Express, Discover, JCB, MasterCard, and Visa.

Payment Card Data
Also referred to as cardholder data (CHD), payment card data refers to any information contained on a customer's payment card. The data is printed on either side of the card and also may be contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded in the front side. At a minimum, payment card data includes the primary account number (PAN), cardholder name, expiration date, and service code.

PCI DSS (Payment Card Industry Data Security Standard)
Security standards developed collaboratively by the major card issuers must be adopted by all merchants that accept payment cards.

Technology Resources
"Technology resources" include:

- any computer or electronic resources used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of Trinity College data;
- any technologies or services owned or managed by the college, that connect to the college network, connect to another college technology or service, or store college data or information; and
- any services or applications used by the college in hosted environments in which the college does not own or operate the technology infrastructure.

Payment Card Acceptance Procedures
Permission to Accept Payment Cards

Approval from Accounting Services is required before any department, unit, or entity may:

- Accept payment cards for donations or as a method of payment,
- Use third-party hardware solutions (i.e., Square, Stripe) to process mobile credit card transactions.

Departments, units, or entities that seek to engage in payment card transactions must seek approval from Accounting Services. Accounting Services will review the request to accept payment cards and will set up merchant accounts for each department, unit, or entity approved to accept payment cards. Departments and organizations may not use peer-to-peer payment solutions such as Venmo to collect payments or donations.

Any department, unit, or entity approved to accept payment cards must:

- Follow procedures and guidelines issued by Accounting Services related to payment card acceptance.
- Limit access to cardholder data to only those individuals whose jobs require such access.
- Ensure that any individuals with access to payment cards or cardholder data complete annual PCI DSS training.

Establishing a Payment Card Account

Departments and individuals who desire to process payment card transactions must coordinate with the Accounting Services Department. Accounting Services will train or update employees on the College policies and procedures of accepting payment cards as needed.

Short-Term Use & Individual Events

For short-term use or individual events, departments and organizations must complete and submit the Payment Card Application Form. Once approved, Accounting Services will issue a College owned credit card reader to be used and returned. The individual who completes the Payment Card Application Form must be the individual to pick up the credit card reader from Accounting Services. Transaction activity will be tracked and recorded to a College owned bank account for the duration of the event and reconciled by Accounting Services. Revenue will be transferred to the departmental or organization account following reconciliation.

Ongoing Credit Card Reader Usage

Departments and organizations must complete and submit the Payment Card Reader Application Form, which is reviewed by Accounting Services. Accounting Services will set up each department merchant account under Trinity College's main bank account, and monitor/reconcile activity as it occurs.

Merchants can clear Visa, MasterCard, and Discover together on a single merchant account. American Express fees are typically higher so Accounting Services will set up separate American Express merchant accounts (if desired).

Departments may be required to provide certain accounting records to Accounting Services for payment card transactions (ex. department code or project code).

Processing Payments

The following procedures must be complied with when accepting payment card payments. Accounting and LITS personnel should be contacted to discuss all specific PCI security issues.

Procedures For Payment Card Payments Over the Internet

Users must use payment gateways that are PCI DSS compliant for receiving, transmitting, and storing payment card data. The transaction information should be collected and securely stored by the payment gateway or processor, so there is no reason for payment card data to be collected or stored on Trinity College computers or networks.

Users should obtain from the payment gateway or processor only the information necessary to apply the payment (such as the name and amount). Users should not retain any files or reports containing payment card data. The full contents of any track data from the magnetic stripe, the card verification code, and the PIN should not be stored under any circumstances. In the event of a dispute or chargeback, Accounting Services can research the transaction on the processor's website via secure login.

Procedures For Payments Where the Card is Present

Payment card equipment must be capable of protecting stored data and encrypting transmitted payment card data. Only PCI PIN Transaction Security (PTS) compliant fully end-to-end encrypted devices may be connected to the Trinity College network. Imprint machines cannot be used.

Payment card information must be truncated to the last 4 digits. The full card number should never be printed on anything, including the customer copy, our copy, or batch reports. In the event of a dispute or chargeback, we can research the transaction on the merchant account website via secure login.

Any receipts or batch reports should never contain the full card number.

Procedures For Payments When the Card is Not Present (via Mail or Phone)

Whenever possible, departments should refer the individual to a secure payment gateway, rather than having them mail payment card information or transmit it to the College over the phone. If it is necessary to have the payment card information in hardcopy, it should be entered promptly and then immediately destroyed by shredding so that cardholder data cannot be reconstructed. Containers storing information waiting to be destroyed must be secured to prevent access to the contents.

Maintaining a Payment Card Account

All employees who handle any payment card information must complete a mandatory annual PCI DSS training program as outlined in the Security & Compliance section. Once Training is assigned, it can be located and completed here.

Departments that manage, handle, and accept payment cards on behalf of the College must report annually to Accounting Services at acctservices@trincoll.edu:

- Their current payment card acceptance procedures
- All personnel handling payment cards

This information should be reported by October 1st on an annual basis.

Accounting Services will notify any departments or organizations with ongoing usage of payment card readers of any changes in the industry and PCI DSS standards.

Security & Compliance

Payment Card Security Standards

Access to payment card information should be limited to only those employees who need the information for their jobs. Any department, unit, or entity approved to accept payment cards is responsible for securing cardholder data, and the cardholder data environment (CDE). Any department, unit, or entity approved to accept payment cards is prohibited from collecting payment card information on the Trinity network, storing any payment card information electronically, or sending payment card information via electronic means (e.g., text, email, chat, instant messaging).

Any department, unit, or entity approved to accept payment cards must:

- Adhere to all applicable PCI DSS requirements published and maintained by the PCI Security Standards Council.
- Follow all policies, standards, procedures, and guidelines issued by Accounting Services and LITS related to payment cards, cardholder data, the CDE, and other information security concerns.
- Ensure that all technology resources which are used to facilitate the acceptance of payment cards are approved by Accounting Services and LITS before entering into any contracts or purchasing any technology solutions or equipment. This includes, but is not limited to, devices, software, payment gateways, payment processors, and other hardware or technologies.
- Immediately report any confirmed or suspected compromise of the CDE or cardholder data to Accounting Services acctservices@trincoll.edu and LITS at security@trincoll.edu.

Mandatory Annual PCI DSS Training Program

Employees that handle any payment card information (physical terminals, virtual terminals, and payment card numbers) must complete a mandatory PCI DSS training program. Completion of training is valid for one fiscal year regardless of the level of usage. Completing the PCI DSS program will help ensure that you are aware of the PCI DSS requirements and the types of attacks used to attempt to steal personal data and compromise your computing devices.

Data Security

Devices used to process credit cards should be used only to process credit card payments. All services not directly needed to perform the device's specified function should be disabled. These devices should only be used in locations where credit card acceptance is necessary and all procedures in this policy can be followed.

Access to cardholder data should be limited to only those individuals whose jobs require such access. Each individual with access to cardholder data should have a unique user ID, when applicable. User IDs should not be shared with other individuals. Approval should be obtained from the appropriate parties (LITS, Business Office, Individual Departments, etc.) to use credit card processing technologies.

Identifying & Reporting Incidents

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Any confirmed or suspected compromise of the cardholder data environment or cardholder data must be immediately reported to Accounting Services AcctServices@trincoll.edu and LITS at security@trincoll.edu.

Some examples of security incidents that an employee might recognize in their day-to-day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g. papers missing from their desk, broken locks, missing log files, an alert from public safety, evidence of a break-in or unscheduled/unauthorized physical entry)

- Fraud – Inaccurate information within databases, logs, files, or paper records

Compliance & Policy Violations
Institutionally, the College also must complete an annual on-site inspection that evaluates an organization's cardholder data environment (CDE) to remain in compliance with PCI DSS. This Self-Assessment Questionnaire (SAQ) is conducted by Accounting Services and overseen by Library & Information Technology Services. The Self-Assessment Questionnaire, once completed, is a formal attestation of compliance.

Any person, department, unit, or entity that transacts business using payment cards in a manner that deviates from this policy is subject to various financial penalties and sanctions. These may include termination of the ability to accept payment cards, financial penalties and costs associated with a security breach or fraudulent transactions, as well as penalties and costs associated with bringing non-compliant applications into scope.

Violations of this policy or any law related to the use of college technology resources or college data, including, but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Gramm Leach Bliley Act (GLBA), may result in disciplinary action in accordance with the Student Handbook, Faculty Handbook, Employee Handbook, as appropriate, and/or any other applicable rules governing employment at Trinity College.

Responsibilities

The roles and responsibilities for payment card acceptance include:

Departments or Units Accepting Payment Cards for Payments

- Comply with this policy and related Accounting Services and LITS procedures.
- Ensure that access to payment card data is restricted to only those employees for whom such access is required to carry out the responsibilities of their position.
- Ensure that all staff with payment card responsibilities complete mandatory PCI DSS training program on an annual basis.
- Follow established College business procedures when making changes to the CDE (i.e., a new purpose for accepting payment cards, new technology resources or applications, etc.).
- Immediately report any confirmed or suspected compromise of the CDE or cardholder data to Accounting Services and LITS.

Accounting Services

- Review requests for approval from departments, units, or entities wanting to accept payment cards.
- Set up merchant accounts for each department, unit, or entity approved to accept payment cards as payment.
- Maintain related business procedures and assess compliance with the procedures by each department, unit, or entity annually.
- Provide compliance reports to the acquiring bank/processor as required.
- In coordination with LITS:
    - Review all contractual agreements for services and equipment that include the acceptance of payment cards.
    - Evaluate and approve new point-of-sale equipment utilized to accept/process payment cards.
    - Develop, review, and update the annual mandatory PCI DSS training program.
    - Respond to reports of confirmed or suspected incidents regarding payment cards.
    - Issue notifications of policy violations to the responsible department/unit, Chief Financial Officer, and responsible division head and implement any necessary changes and subsequent penalties.
    - Keep abreast of changes in the industry and PCI DSS standards
    - Complete the Self-Assessment Questionnaire (SAQ) on an annual basis

Library and Information Technology Services

- Establish related technical standards.
- Conduct compliance validation and assessment services.
- Coordinate technical oversight to ensure new implementations of any changes to existing applications and their related hardware are compliant with the current applicable PCI DSS requirements.
- Distribute annual Self-Assessment Questionnaires to departments collecting payment card information.
- Conduct a review to assess risk and identify systemwide vulnerabilities at least quarterly or when the cardholder environment changes.
- In coordination with Accounting Services:
    - Review all contractual agreements for services and equipment that include the acceptance of payment cards.
    - Evaluate and approve new point-of-sale equipment utilized to accept/process payment cards.
    - Develop, review, and update the annual mandatory PCI DSS training program.
    - Respond to reports of confirmed or suspected incidents regarding payment card data.

- Issue notifications of policy violations to the responsible department/unit, Chief Financial Officer, and responsible division head and implement any necessary changes and subsequent penalties.
- Keep abreast of changes in the industry and PCI DSS standards
- Oversee and review the Self-Assessment Questionnaire (SAQ) on an annual basis

Cross References to Related Policies
College Policies
Library & Information Technology Policies, Procedures & Standards

Responsible Officer
Vice President of Finance and Chief Financial Officer

Key Offices to Contact Regarding the Policy and Its Implementation
Questions or clarifications regarding this policy should be directed to Accounting Services.

Confirmed or suspected compromise of the CDE or cardholder data must be reported immediately to Accounting Services and LITS: security@trincoll.edu

Links to Procedures or Forms
Additional information related to Accounting Services can be found at:

Trinity College Accounting Services

Information Technology Policies and Procedures can be found at**:**

Payment Card Reader Application Form

This policy was issued on October 1, 2025