Policy Chapter:	**Chapter 10 Fiscal Management**
Policy Number and Title:	**10.035 Accepting Credit Cards**

I. Policy Statement

UNT supports the acceptance of credit cards as payment for goods and services to improve customer service, bring efficiencies to the university's cash collection process, and increase the sales volume of certain types of transactions. UNT requires that all units that accept credit cards do so only in compliance with the Payment Card Industry Data Security Standards (PCI DSS), and in accordance with this policy.

II. Application of Policy

All University faculty, staff, and third-party service providers.

III. Policy Definitions

A. Department Designee

"Department Designee," in this policy, means an employee who has been authorized by the department account holder to accept payment cards.

B. Department Account Holder

"Department Account Holder," in this policy, means the employee with management responsibility for financial transactions for the Department which the employee is the Holder of Record, as set forth in UNT Policy 10.005, Department Holder and Project Holder Responsibility.

C. Merchant

"Merchant," in this policy, means a unit, department, or college which processes credit card transactions as a method of payment.

D. Merchant ID

"Merchant ID," in this policy, means a unique identification number issued by the Merchant Bank/Payment Processor and used to identify the unit, department, or college when processing credit cards.

E. Merchant Bank/Payment Processor

"Merchant Bank/Payment Processor," in this policy, means a bank or financial institution that processes credit and/or debit card payments on behalf of the University. The same institution can also be the issuer of merchant ID's to University merchants. Annual Compliance to the PCI DSS is validated directly to this entity.

F. Payment Card Industry Data Security Standards (PCI DSS)

"PCI DSS," in this policy, means a set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council (PCI SSC) to help facilitate the broad adoption of consistent data security measures on a global basis.

G. Payment Card

"Payment Card," in this policy, means support for cashless payment for goods and services. Examples include, but are not limited to, credit cards, debit cards, and reloadable prepaid cards.

H. Third Party Service Provider (TSP)

"Third Party Service Provider," in this policy, means a business entity which is directly involved in the processing, storage, or transmission of cardholder data on behalf of another business. This also includes companies that provide services that control or could impact the security of cardholder data.

I. Self –Assessment Questionnaire (SAQ)

"SAQ," in this policy, means a validation tool intended to assist a merchant and third-party service provider(s) in self-evaluating their compliance with PCI DSS.

IV. Policy Responsibilities

A. Payment Card Processor

All payment card transactions must go through the University's approved and contracted merchant bank/payment card processor. Any exceptions should be directed to University Integrity and Compliance (UIC) in order to assess its compliance and approval.

B. Methods of Processing

The following are acceptable methods of credit card payment processing:

1. Physically

   This is done through a point-of-sale terminal procured through UNT's merchant bank. If a PCI SSC validated Point-to-Point Encryption (P2PE) solution is available, it must be used unless an exception is granted by UIC.

2. Online

   This is done through an approved and previously assessed online e-commerce processor solution. Any exceptions to this must be reviewed and approved by UIC.

3. Mobile

   Processing payment cards through mobile networks or mobile devices must be reviewed and approved by UIC to ensure that all appropriate data security standards are met.

4. Telephone

   If accepting payment cards over the telephone, secure processes must be followed on how card holder data is handled, processed for payment, and disposed. These processes must be reviewed and approved by UIC to ensure that all appropriate data security standards are met.

5. Mail or Fax

   Receiving and processing payment cards through the mail or fax is highly discouraged. However, if there is no other alternative, secure processes must be followed on how card holder data is handled, processed for payment, and disposed. These processes must be reviewed and approved by UIC to ensure that all appropriate data security standards are met.

6. E-mail

   Receiving and processing payment cards through email is strictly prohibited.

C. Acceptable Third-Party Service Providers

1. If using a third-party system to process payment cards, it must be reviewed and approved by UIC before procurement of the system.
2. Only PCI DSS compliant vendors may be used. Proof of compliance must be:
   a. an AOC (Attestation of Compliance) from the TSP with a validation date within the last 12 months; or
   b. a written agreement or statement from the third-party service provider acknowledging their responsibility for the security of card holder data they possess and process. This can be a written document or be included as part of the TSP contract.
3. Each TSP must go through a revalidation process annually in order to comply with the PCI DSS requirement.
4. Each department is responsible for obtaining the required documentation in order to revalidate each of their third-party service providers.

D. Establishing and Maintaining a Merchant Account

1. UIC is responsible for managing all aspects of establishing payment card merchants on campus. UIC is responsible for consulting and advising departments on the technical requirements for accepting payment cards. The procedure to request approval to accept payment cards is established in the Payment Card Merchant Feasibility Questionnaire.
2. Each department account holder is responsible for establishing controls to ensure separation of duties.
3. The department account holder or designee(s) must perform credit card transaction reconciliations and reconciliation documentation in accordance with their department's written procedures as described in UNT Procedures for Cash Handling

Control.

4. All sales and goods of services must comply with UNT Policy 10.024, Sale and Receipt of Funds.

5. All credit card transactions must be processed through the appropriate credit card terminal or credit card system as instructed and approved by UIC.

E. Compliance and Training

1. PCI DSS Awareness training is required annually for the following personnel:

    a. any employees who process payment cards or have access to sensitive payment card information;

    b. supervisors of the above employees; and

    c. any newly hired employees or any current employees (part-time or full-time) whose function may include processing payment cards or handling sensitive payment card information.

2. Prior to accepting payment cards and annually thereafter, the department account holder and all department designees must adhere to the following requirements:

    a. attend cash control training in accordance with UNT Policy 10.006, Obtaining and Controlling Cash Funds;

    b. complete the PCI DSS Awareness training; and

    c. complete the annual SAQ as required.

3. The above requirements must also be completed every year after the initial validation year in order to continue accepting credit cards.

F. Authority and Responsibilities

1. Department account holders and/or department designee(s) that accept payment cards are responsible for:

    a. following the specific security standards set forth in the PCI DSS; all applicable policies set forth in UNT Policy 14.002, Information Security; and the established data protection rules detailed in the accompanying procedure document to this policy;

    b. responding to card brand chargebacks, disputes, sales draft retrieval requests, or other requests from the merchant bank or cardholder within the specified time period;

    c. notifying UIC, and the IT Shared Services (ITSS) information security team of any security lapse on the date the lapse is realized. ITSS information security team is responsible for investigating security breaches in accordance with UNT Policy

14.002, Information Security. Departments are responsible for implementing timely corrective measures, including remediating security issues; and

   d. participating in and completing the annual SAQ as required per PCI DSS.

2. UIC is responsible for:

   a. obtaining payment card merchant IDs in coordination with the merchant bank;

   b. performing periodic and annual assessments to ensure compliance with the requirements outlined in this policy and the PCI DSS;

   c. verifying all merchants are in compliance with university policies and current PCI DSS controls in regards to protecting cardholder data;

   d. providing annual or "on-the-spot" training in order to satisfy authorization requirements;

   e. coordinating the annual compliance validation process in coordination with the merchant bank's security assessor; and

   f. recommending the revocation of the ability to accept credit cards for any department that fails to comply with the PCI DSS and/or this policy. Departments, department account holders, and department designees who fail to comply with this policy may have their payment processing privileges revoked. Department account holders and department designees may be subject to disciplinary action up to and including termination in accordance with UNT Policy 05.033, Staff Employee Discipline and Discharge.

3. ITSS, Administrative IT and Academic IT are responsible for:

   a. assisting UIC and merchants in assessing its payment card processes and applications, as well as migration to a PCI DSS compliant solution as needed; and

   b. providing technical assistance to UIC as well as verifying requirements with the current PCI DSS, to include: terminals, mobile devices, workstations, firewalls, and any other network component as part of the card holder data environment.

4. All documents created to comply with this policy must be maintained in accordance with UNT Policy 04.008, Records Management and Retention.

V. Resources/Forms/Tools

New User Statement of Understanding
UNT Payment Merchant Security Agreement
Establishing a Campus Merchant Account Procedure
Payment Card Merchant Feasibility Questionnaire

VI. References and Cross-References

PCI Security Standards Council
UNT Employee Portal
UNT Policy 04.008, Records Management and Retention
UNT Policy 05.033, Staff Employee Discipline and Involuntary Termination
UNT Policy 10.005, Department Holder and Project Holder Responsibility
UNT Policy 10.006, Cash Handling Controls
UNT Policy 10.024, Sales and Receipt of Funds
UNT Policy 14.002, Information Security
UNT Procedures for Cash Handling Control

VII. Revision History

Policy Contact:	Director, PCI Compliance & Merchant Services
Approved Date:	08/01/1999
Effective Date:	10/11/2018
Revisions:	04/2000, 05/2001, 04/2006, 05/2008, 01/12/2017, 10/11/2018, 12/01/2023