Policies of the University of North Texas	Chapter 10
10.035 Accepting Credit Cards	**Fiscal Management**

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 the procedures outlined in this document.

Application of Policy. All University faculty, staff, and third party service providers.

Definitions.

1. E-Commerce Processor. "E-Commerce Processor" means a department that is established within the University's contracted and approved electronic commerce payment solution.
2. Department Designee. "Department Designee" means an employee who has been authorized by the department account holder to accept payment cards.
3. Department Account Holder. "Department Account holder" means the employee with management responsibility for financial transactions for the Department for which he/she is the Holder of Record, as set forth in UNT Policy 10.005.
4. Merchant. "Merchant" means a unit, department or college which processes credit card transactions as a method of payment.
5. Merchant ID. "Merchant ID" means a unique identification number issued by the Merchant Bank/Processor and used to identify the unit, department or college when processing credit cards.
6. Merchant Bank/Payment Processor. "Merchant Bank/Payment Processor" 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 issue of merchant ID's to University merchants. Compliance to the PCI DSS is validated directly to this entity.
7. Payment Card Industry Data Security Standards (PCI DSS). "PCI DSS" means a set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.
8. Payment Card. "Payment Card" means support for cashless payment for goods and services. Examples include, but are not limited to, credit cards, debit cards, and reloadable prepaid cards.
9. Third Party Service Provider. "Third Party Service Provider" 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.

10. Self –Assessment Questionnaire (SAQ). "SAQ" means a validation tool intended to assist a merchant and third party service provider(s) in self-evaluating their compliance with PCI DSS.

Procedures and Responsibilities.

I. Payment Card Processor.

A. All payment card transactions **must** go through the University's approved and contracted merchant bank/payment card processor. Any exceptions should directed to the Asset Protection Unit ("APU") in order to assess its compliance and approval.

II. Methods of Processing. The following are acceptable methods of credit card payment processing.

A. Physically: This is done through a point of sale terminal procured through UNT's payment card processor. If a PCI SSC validated P2PE solution is available, it must be used unless an exception is granted by the APU in the division of Finance and Administration.

B. Online: This is done through UNT's online e-commerce processor solution. Any exception to this must be reviewed by IT Shared Services (ITSS) information security team and Administrative Information Technology Services (AITS) or College Information Technology (CIT) as applicable. Approval for the exception will be granted by the APU.

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

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

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

F. E-mail: Receiving and processing payment cards through email is strictly prohibited.

III. Acceptable Third Party Vendors.

A. If using a third party software to process payment cards, the software must connect through the University's e-commerce solution. Any exception to this must be reviewed

by the following groups: ITSS, and AITS or CIT as applicable. Approval for the exception will be granted by the APU.

B. Only PCI DSS compliant vendors may be used. Proof of compliance must be:

(1) An AOC (Attestation of Compliance) from the third party service provider with a validation data within the last 12 months.

(2) 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 vendor contract.

C. Each vendor will go through a revalidation process annually in order to comply with the PCI DSS requirement.

D. Each department is responsible for obtaining the required documentation in order to revalidate each of their third party service providers.

IV. Establishing and Maintaining a Merchant Account.

A. The APU is responsible for managing all aspects of establishing payment card merchants on campus and processing payment card transactions. The APU 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 accompanying process document.

B. Each department account holder is responsible for establishing controls to ensure separation of duties.

C. The department account holder or designee(s) must perform daily reconciliations of the credit card transactions on the days that transactions occur and must retain documentation of those reconciliations in accordance with UNT Policy 10.006.

D. All sales and goods of services must comply with UNT Policy 10.024.

E. All credit card transactions **must** be processed through the appropriate credit card terminal or software package as instructed and approved by the APU.

Responsible Parties: Department Designee(s), Department Account Holder, Asset Control Director, Asset Protection Executive Director

V. Compliance and Training.

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

(1) Any employees who process payment cards or have access to sensitive payment card information

(2) Supervisors of the above employees

B. 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.

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

(1) Attend cash control training in accordance with UNT Policy 10.006

(2) Complete the PCI DSS Awareness training and pass the PCI DSS quiz

(3) Complete the annual Self-Assessment Questionnaire (SAQ)

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

VI. Authority and Responsibilities.

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

(1) Following the specific security standards set forth in the PCI DSS, all applicable policies set forth in UNT Policy 14.002, and the established data protection rules detailed in the accompanying procedure document to this policy.

(2) Responding to card brand chargebacks, disputes, sales draft retrieval requests or other requests from the merchant bank or cardholder within the specified time period.

(3) Notifying the APU, and the 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. Departments are responsible for implementing timely corrective measures, including remediating security issues.

(4) Participating in and completing the annual Self-Assessment Questionnaire (SAQ) as required per PCI DSS.

Responsible Parties: Department Designee(s), Department Account Holder, Asset Control Director, Asset Protection Executive Director, ITSS Information Security, AITS and CIT.

B. The APU is responsible for:

(1) Obtaining payment card merchant ID's in coordination with the merchant bank.

(2) Performing periodic and annual assessments to ensure compliance with the requirements outlined in this policy.

(3) Verifying all merchants are in compliance with University policies and current PCI DSS controls in regards to protecting cardholder data.

(4) Providing annual or "on-the-spot" training in order to satisfy authorization requirements.

(5) Coordinating the annual compliance validation process in coordination with the merchant bank's security assessor.

(6) 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.

Responsible Parties: Department Designee(s), Department Account Holder, Asset Control Director, Asset Protection Executive Director

C. ITSS information security, AITS and CIT are responsible for:

(1) Assisting merchants in assessing its payment card processes, applications, and migration to a PCI DSS compliant solution and in consultation with the APU.

(2) Providing technical assistance to the APU 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.

D. The Student Financial Services Cashiering Manager or its designee is responsible for communicating with departments when there are chargebacks, disputes, sales draft retrieval requests or other requests from the merchant bank or cardholders.

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

Responsible Parties: Department Designee(s), Department Account Holder, Cashiering Manager, Asset Control Director, Asset Protection Executive Director, Vice President of Finance or Designee

References and Cross-references.

PCI Security Standards Council
UNT Employee Portal
Establishing a Campus Merchant Account Procedure
Policy 04.008, Records
UNT Policy 04.008, Records Management and Retention
UNT Policy 05.033, Staff Employee Discipline and Involuntary Termination
UNT Policy 10.005, Accountholder Responsibility
UNT Policy 10.006, Cash Handling Controls
UNT Policy 10.024, Sales and Receipt of Funds
UNT Policy 14.002, Information Security

Forms and Tools.

New User Statement of Understanding

UNT Payment Merchant Security Agreement

Approved: 08/01/1999
Effective: 10/11/2018
Revised: 04/2000; 05/2001; 04/2006; 05/2008; 03/2011*; 01/12/2017; 10/11/2018
*format only