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 credit card industry standards, specifically Payment Card Industry Data Security Standards (PCI DSS), and in accordance with the procedures outlined in this document.

Application of Policy. All University.

Definitions.
1. **Commerce Manager Processor.** “Commerce Manager Processor” means a department that is established within Commerce Manager.
2. **Department Designee.** “Department Designee” means an employee who has been authorized by the Dept ID holder to accept payment cards.
3. **Department Identification Holder (Dept ID Holder).** “Dept ID 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 that accepts payment cards as a method of payment.
5. **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.
6. **Payment Card.** “Payment Card” means a debit or credit card.

Procedures and Responsibilities.
1. **Establishing a Merchant Account.**
   A. Student Accounting and University Cashiering Services (SAUCS) is responsible for managing all aspects of establishing payment card merchants on campus and processing payment card transactions. IT Shared Services Information Security Team (ITSS team) is responsible for consulting and advising departments on the technical requirements for accepting payment cards. To request approval to accept payment cards, the Dept ID holder must contact SAUCS. Departments that will process payment cards on a regular basis may be set up as a merchant. Departments that will process payment cards on an infrequent basis may be set up as a commerce manager processor. SAUCS will review and approve each request based on the consultation
from ITSS and make the determination for how the department’s payment processing will be set up. Departments are responsible for implementing and maintaining security requirements established in PCI DSS.

B. The Dept ID holder is responsible for establishing controls to ensure separation of duties such as requiring that the department designee entering payments is not the same person responsible for reporting. In accordance with UNT Policy 10.006, departments must establish written internal procedures for separation of duties.

C. The Dept ID holder or designee 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. The Dept ID holder is prohibited from negotiating directly with the university’s depository bank or a payment card company to set up a credit card merchant agreement/contract.

F. All credit card transactions must be processed through the appropriate credit card terminal or software package as instructed by SAUCS and approved by the ITSS team. All credit card transactions and processes/procedures are subject to the guidelines set forth in the UNT Payment Card Merchant Handbook, and are subject to review by Internal Audit.

   Responsible Party: Department Designee, Dept ID Holder, SAUCS Cashier Area Supervisor, ITSS Team Manager or Designee, Internal Audit

II. Credit Card Data Protection.


B. The Dept ID holder or department designee must notify SAUCS and the ITSS team of any security lapse on the date the lapse is realized. SAUCS and the ITSS Team is responsible for investigating security breaches in accordance with UNT Policy 14.002. Departments are responsible for implementing corrective measures, including remediating security issues.

   Responsible Party: Department Designee, Dept ID Holder, SAUCS Cashier Area Supervisor, ITSS Team Manager or Designee

III. Compliance and Training.

A. Prior to accepting payment cards and annually thereafter, the Dept ID holder and all department designees must attend cash control training in accordance with UNT Policy 10.006, must complete a UNT Payment Merchant Security Agreement, and must pass the PCI Quiz. Dept ID holders are responsible for ensuring their locations are following the policies set forth herein, the guidelines set forth in the UNT Payment Card Merchant Handbook, and the Payment Card Industry Data Security Standards.
B. SAUCS is responsible for performing annual reviews to ensure compliance with the requirements outlined in this policy.

C. Departments are responsible for participating in and completing annual assessments as required per PCI DSS and SAUCS.

D. Departments, Dept ID holders, and department designees who fail to comply with this policy may have their payment processing privileges revoked and Dept ID holders and department designees may be subject to disciplinary action up to and including termination in accordance with UNT Policy 05.033.

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

F. The division of Finance and Administration will provide annual training in order to satisfy authorization requirements. Training registration will be available within the university’s employee portal.

   Responsible Party: Department Designee, Dept ID Holder, SAUCS Cashier
   Area Supervisor or Designee, Vice President of Finance or Designee

References and Cross-references.

PCI Security Standards Council
UNT Employee Portal
UNT Payment Card Merchant Handbook
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 Policy
UNT System Payment Card Processing Procedures

Forms and Tools.

New User Statement of Understanding
UNT Payment Merchant Security Agreement

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