

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

Policy Statement.

Application of Policy. Total University.

Procedures and Responsibilities. Departments interested in accepting credit card payments should contact the Cashier Area of Student Accounting and University Cashiering Services in the Eagle Student Services Center to receive information regarding procedures to initiate a credit card merchant application and agreement.

An application and agreement must be completed and approved before credit card payments may be accepted by a department. Campus departments are not authorized to negotiate directly with the University’s depository bank or a credit card company to set up a credit card merchant agreement/contract. This process is centralized on campus in the area of Student Accounting and University Cashiering Services. Centralization of credit card agreements allows the University CITC security team to monitor all merchants for PCI DSS (Payment Card Industry Data Security Standards) compliance. It also allows the University to obtain the lowest possible discount rate with each credit card company for all departments. An informational handbook listing all the guidelines will be provided by Student Accounting and University Cashiering Services.

All credit card transactions must be processed through the appropriate credit card terminal or software package as instructed by Student Accounting and University Cashiering Services and approved by the CITC security team. Any department wanting to accept credit cards through the internet (web application) must contact Student Accounting and University Cashiering Services to receive information and pricing for the eCommerce provider and payment processor under contract with the University. Student Accounting and University Cashiering Services along with the CITC security team will facilitate the initial implementation phase of the eCommerce product. All credit card transactions and processes/procedures are subject to review by Internal Audit.

In an effort to maintain consistency and to provide better customer service campus-wide, departments approved to accept credit card payments must honor all of the four major credit cards (MasterCard, Visa, Discover and American Express).

If you have any questions regarding credit card payments, please contact Student Accounting and University Cashiering Services at (940) 565-3387.

Responsible Party: Student Accounting and University Cashiering Services

- I. **Credit Card Data Protection.** A university department processing credit card information must follow specific security rules/standards (Payment Card Industry Data Security Standards –PCI DSS) instituted by Mastercard and Visa. These rules are designed to prevent abuse of the data and protect the consumer from some forms of identity theft. Failure to follow these requirements can involve severe penalties, including fines to the

University and prohibition from further acceptance of credit cards. The requirements for protecting credit card data are described in detail in the UNT Credit/Debit Card Merchant Handbook.

Please reference Information Security Policy 3.6 for more information regarding the use of and security of information resources as it applies to PCI DSS.

- II. Compliance Certification. The Dept ID/Proj ID holder and department designee will be required to attend credit card training annually. A department designee is anyone in the department who can process credit card transactions. Training will include attendees signing an agreement stating they will comply with policy and procedure in regards to Payment Card Industry Data Security Standards (PCI DSS) requirements. The DeptID/ProjID holder will be responsible for insuring their location (merchant) is following the University credit card guidelines including PCI Data Security Standard (PCI DSS) requirements.

Responsible Party: DeptID/ProjID holder

- III. Disclosing Security Breaches. If credit card information is compromised the DeptID/ProjID Holder or department designee should immediately contact the CITC security team, their network manager and the Cashier Area Supervisor in Student Accounting and University Cashiering Services.

Responsible Party: DeptID/ProjID Holder, Student Accounting and University Cashiering Services

References and Cross-references.

Payment Card Industry Data Security Standards
UNT Policy 3.6, Information Security Policy

Approved: 8/1/1999

Effective: 5/1/2008

Revised: 4/00; 5/01; 4/06; 05/08;

*3/2011 format only