Payment Card Processing Procedures

Purpose
This document outlines the requirements for payment card acceptance and processing by any department or organization of the UNT System Administration and its Institutions. The purpose of these procedures is to ensure the integrity of cardholder data and adherence to Payment Card Industry Data Security Standards.

Scope
These procedures apply to any department or organization of the UNT System Administration and its Institutions that accept credit card payments or handle cardholder data.

Procedure
Any department or organization of the UNT System Administration or any of its Institutions interested in accepting credit card payments should contact the Student Accounting and University Cashiering Services to initiate a credit card merchant application and agreement. All departments accepting credit card transactions are merchants and therefore, must be in compliance with the credit card policy of its institution and the Payment Card Industry Data Security Standards (PCI DSS).

The PCI DSS applies to any merchant that accepts or processes payment cards. The PCI DSS covers twelve domains, each with multiple components, that align with best practices of security. The twelve domains are:

1. Establish and maintain a firewall
2. Do not use vendor-supplied defaults for security
3. Protect stored cardholder data
4. Encrypt cardholder data that is transmitted across public networks
5. Establish and maintain secure systems and applications
6. Restrict access to cardholder data to a need-to-know basis
7. Provide a unique ID for everyone requiring access
8. Restrict physical access to cardholder data
9. Track and monitor all access to cardholder data
10. Regularly test security systems and processes
11. Maintain a policy that addresses information security for all personnel.

All merchants should work with the Student Accounting and University Cashiering Services of their institution, their departmental network manager and ITSS Information Security to resolve any compliance concerns.

A part of PCI DSS requirements is to complete an annual Self-Assessment Questionnaire (SAQ) and attestation of compliance. Merchants found to be out of compliance may lose the right to accept credit cards until compliance has been established. Additionally, in the event of a breach, organizations out of compliance could be levied significant fines by the individual payment card brands.

Created: 6/18/2013
Updated: 6/18/2013

References

PCI Security Standards Council
UNT Payment Card Merchant Handbook, Student Accounting and University Cashiering Services
UNT Policy Office, Accepting Credit Cards (2.2.31)
Fiscal Manual, University of North Texas Health Science Center at Fort Worth

Contact Information

Information Security Team
IT Shared Services
http://security.untsystem.edu
security@untsystem.edu
(940) 369-7800

Created: 6/18/2013
Updated: 6/18/2013