Policy Statement

Purpose

The University has adopted the following policy for all types of credit card transactions. The purpose of this policy is to protect the interests of the University and its customers by establishing strong internal business controls and standard revenue collection methods throughout the University.

This policy provides guidance so that the processes of accepting electronic payments comply with the Payment Card Industry Data Security Standards (PCI DSS) and are appropriately integrated with the University's financial and other systems. In addition, adherence to this policy will ensure compliance with Sections 72.004 and 502.002 of the Texas Business & Commerce Code, related to the protection of credit/debit card information and other personal identifying information.

Applicability

Any UT Dallas employee, contractor, or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit card or electronic payments is subject to this policy. Failure to comply with the terms of this policy may predispose the department and/or the University to financial losses and/or legal liabilities.

Effective Date

March 3, 2020

Policy Ownership

Vice President of Budget and Finance

Policy Statement

Any department collecting electronic payments via the web on behalf of the University for goods or services must utilize a secure web based storefront. The Office of Budget and Finance (OBF) has selected a designated vendor for this service, which allows secure payment via credit card or check. If a department believes that it has a significant business case or processing requirement that cannot be achieved using the designated vendor it may be granted an exception to use other credit card processing systems.

Any department accepting credit/debit cards from patrons in person must also use one of OBF's designated vendors, unless an exception is granted.

Responsibilities of a Merchant Department

The following responsibilities are an important aspect of the University's compliance with the PCI Data Standards. Any department collecting revenue on behalf of the University is considered a Merchant Department. The Merchant Department must designate an individual who will have primary authority and responsibility for revenue collection within that department. This individual will be the designated Merchant Department Representative or "MDR".

All Merchant Departments must:

1. Follow OBF procedures to become a Merchant Department.
2. Follow the Card Acceptance guide (or similar rules) of the merchant processor/acquirer (e.g., Global Payments) and the operating regulations and rules of any card associations/networks that will be accepted by the Merchant Department (e.g., MasterCard, Visa, etc.). These can be found on the OBF website: (link forthcoming)
3. Ensure that all employees, including the MDR, contractors and agents with access to payment card data complete compliance training on an annual basis.
4. Ensure that no credit/debit card receipt or other physical or electronic document created or maintained by UT Dallas that references the transaction include the full credit/debit card account number.
5. Ensure that all credit/debit card data collected, regardless of how it is stored and including but not limited to account numbers, card imprints, and Terminal Identification Numbers, is secured in accordance with ISO standards for storing credit card data.
6. Contact Treasury and the Information Security Office if a security incident is suspected. The Information Security Office will provide further instructions that will include measures that will preserve electronic evidence.

No University employee, contractor or agent who obtains access to credit/debit card or other personal payment information may sell, purchase, provide, or exchange said information in any form to any third party other than to the University's acquiring bank, depository bank, credit card company, or pursuant to a government request.

Exception to Using Designated Vendors

If a department believes that it has a significant business case or processing requirement that cannot be achieved using the University's designated vendors, they must provide the details of their case, in writing.

Treasury will review the department's request and consult the Chief Business Officer for approval. In the event that the use of an alternate vendor is approved, the Merchant Department will be subject to periodic inspections by Treasury to ensure compliance with the University policy and the PCI Data Security Standards.

Related Links

PCI Data Security Standards
Texas Business & Commercial Code, Subchapter A, Chapter 72
UT System Information Use and Security Policy - UTS165
Texas Business & Commercial Code, 502.002

Policy History

- Issued: 2009-05-05
- Editorial Amendments: 2014-12-15
- Editorial Amendments: 2019-03-01
- Revised: 2020-03-03

Policy Links

- Permalink for this policy: https://policy.utdallas.edu/utdbp3035
- Link to PDF version: https://policy.utdallas.edu/pdf/utdbp3035
- Link to printable version: https://policy.utdallas.edu/print/utdbp3035