TEMPLE UNIVERSITY
OFFICE OF FINANCIAL AFFAIRS
POLICIES AND PROCEDURES

Title: Electronic Commerce Policy
Policy Number: TBD
Issuing Authority: Office of the Bursar
Responsible Officer: Assistant Vice President and Bursar

Date Created: December 1, 2013
Date Last Amended/Reviewed: n/a
Date Scheduled for Review: December 1, 2015
Reviewing Office: Bursar's Office

Scope of Policy & Rationale:

This policy sets forth guidelines and requirements for the use of electronic commerce. This policy applies to all financial transactions performed using an electronic medium only.

Definitions:

"Electronic Commerce" commonly known as "e-commerce," is defined as the buying and selling of products or services over electronic systems such as the internet.

"Front End Website" refers to an application designed by University staff or a third party vendor to capture consumer demographic and registration data.

"Payment Gateway" is defined as an application service provider which automates the online payment transaction. A payment gateway facilitates the secure encrypted transfer of sensitive information, such as credit card numbers, between the customer and merchant as well as between the merchant and payment processor.

"Credit Card Payment Processor" is the third party provider that authorizes the credit card transactions. The credit card payment processor receives transaction requests from the payment gateway and in real-time, verifies the card details and processes the transaction.

"PCI Compliance" is commonly known as the Payment Card Industry Data Security Standards (PCI DSS). It is a proprietary information security standard for organizations that handle cardholder information for the major debit and credit cards.

Policy Statement:

I. Authorization

All new e-commerce activities must be reviewed and approved by the Director of E-commerce in the Bursar's Office. The review and approval by the Computer Information Security Office (CISO) will also be required in certain situations.

Existing e-commerce activities also may be subject to periodic review by the Bursar's Office and/or Internal Audits to assure compliance with pertinent federal and state statues and regulatory guidelines and requirements.

II. Policy Text

No new e-commerce initiatives and activities shall be established without the proper approval from the Director of E-commerce.

All e-commerce activities must adhere to the University standards and conform to the University's existing e-commerce business model. This includes already approved vendors with which the University has an established contract.

University departments are not permitted to capture, store or transmit payment/credit card information on Temple servers or through the Temple network. All credit card payment processing must be outsourced to an approved third party vendor that is compliant with Payment Card Industry (PCI) Data Security Standards.

University departments may build a front-end website to gather necessary demographic and registration data or may utilize a third party vendor for this purpose. All web applications must go through a pre-production security review before going live. The front-end website must be integrated with a University-approved payment gateway and credit card payment processor. Other non-University supported payment gateways and/or credit card payment processors (such as PayPal) are not permissible.

Any University department offering a non-credit course, event, conference, etc. should consult with the Office of Non-Credit and Continuing Education, which provides an approved online registration and payment capability.

III. Exclusions

The University contracts with credit card payment processors to secure the best possible rates and assure compliance with security and other regulatory requirements.

Because there may be cases where a vendor has both a front-end website for registration and serves as their own payment gateway, the Bursar's Office may grant an exception in these situations if the payment gateway is compatible with the University's credit card payment processor. This exclusion does not apply to any vendor who integrates their product with another payment gateway requiring the University to enter into a duplicate business relationship.

The CISO must review the vendor's product to ensure sensitive data and payment/credit card information is not captured, stored or transmitted via Temple servers or the Temple network. The CISO also will ensure that the vendor is PCI compliant and meets all other required standards.

Notes

1. Dates of official enactment and amendments:

TBD

2. History:

The historical information for this policy is not available as policy was created before a history requirement was created.

Reviewed By:

Assistant Vice President & Bursar & Chief Information Security Officer

3. Cross References/Appendix of University Policies:

Cash Handling (05.20.12)
Credit Card Handling and Acceptance (05.20.17)
Technology Usage (04.71.11)
Comprehensive Information Security Program (04.72.11)