ELECTRONIC COMMERCE POLICY

SCOPE
This policy governs the use of electronic commerce at Duke University and applies to all Duke departments, units, and entities that generate revenue through fundraising or the provision of goods or services. This policy was approved by the Assistant Vice President for Treasury and Cash Management, the Vice President for Information Technology and Chief Information Officer, and the Executive Vice President.

PURPOSE
Electronic commerce provides a convenient way to handle business transactions such as conference registration, donations, or the purchase of goods. Reasonable steps must be taken to protect the privacy of purchasers and to provide security of Duke’s financial transactions. It is also in Duke’s best interest to facilitate the transfer of electronic commerce transaction data to its financial systems. The purpose of this policy is to establish guidelines and standards for electronic commerce.

DEFINITION
For purposes of this policy, electronic commerce is defined as the use of electronic ordering and payment applications via the Internet to effect remote payment for Duke University goods, services, and/or donations, generally between individuals and Duke departments.

This policy does not cover business-to-business e-commerce in which Duke purchases goods or services or to electronic ordering and payment applications that are typically used between other businesses or institutions and Duke, usually referred to as Electronic Data Interchange (EDI) or Electronic Funds Transfer (EFT).

POLICY
Any use of electronic commerce at Duke must be related to the University’s mission of education, research, and health care. In addition, any use of electronic commerce at Duke for the sale of goods and services must conform to Duke Policy #D-70 “Sales of Goods and Services,” which prohibits the Duke community from engaging in businesses unrelated to Duke’s tax-exempt purpose. Sales of goods and services to persons and organizations outside the University community may raise legal, tax, accounting, and community relations considerations; therefore, careful consideration must be given whenever an opportunity is presented to make such sales.

Duke has developed internal e-commerce policies and procedures, called “DukePay”. DukePay is the required application for electronic commerce. DukePay uses a central e-commerce service provided by an authorized internet commerce transaction services vendor to handle the authorization and management of electronic orders. DukePay allows the University to:

- Ensure transactions are transmitted and managed securely as in accordance with the Payment Card Industry Data Security Standard (PCI).
- Eliminate storing any sensitive payment information (i.e. credit card numbers) locally on Duke servers.
- Ensure appropriate integration with University financial systems.
- Ensure compliance with Duke’s name use and privacy policies.
- Use tested emergency response and recovery procedures.
- Leverage University transactions to reduce costs, and
- Provide current technology and support for developing applications.
Other specific policies related to operating an electronic commerce site at Duke are:

- Departments accept financial responsibility for their Internet merchant account(s) and are responsible for all transaction management and reconciliation.
- Departments operating a DukePay site incur the related credit card merchant fees, and are prohibited from charging the end-consumer convenience fees to recuperate such administrative/banking fees.
- Departments accept responsibility for implementing the appropriate internal controls and segregation of duties.
- University departments may not use credit cards to accept payments for a student's Bursar account.

**PROCEDURES / IMPLEMENTATION GUIDELINES**

1. Departments wishing to engage in electronic commerce are required to use DukePay, and should first contact Duke’s Treasury and Cash Management Office to submit their departmental e-commerce business plan and apply for the associated Internet merchant account(s). This information will be reviewed by TCM and depending on the complexity of the issues related to your specific business, you may be asked to make a presentation to the E-Commerce Review Board for final approval. A TCM representative will assist you in preparing for this meeting.

2. Treasury and Cash Management will review all business plans and consult the E-Commerce Review Board when necessary. Due consideration must be given to the sale of goods or services to persons and organizations outside the University community that may raise special considerations (e.g. tax, accounting, legal, etc.). Approval must be granted by the Deputy Treasurer before implementation of an e-commerce enabled website.

3. Departments are responsible for creating their own website “storefront” and integrating to the DukePay payment system. Technical instructions and documentation will be provided to each department. Duke e-Commerce operations must meet the Payment Card Industry Data Security Standard (PCI-DSS). Additional assistance on setting up and running an electronic commerce store is available on the E-Commerce @ Duke site. Departments should work with representatives of the E-Commerce Office, their applications development support team, or other approved constituents to create their electronic commerce-enabled website. References for fee-based technical assistance in creating the department’s electronic commerce-enabled website are available from OIT.

4. Any arrangements with external vendors must be in accordance with Duke Policy #IX.290, Negotiation & Acceptance of Agreements with External Entities.

5. Departments will adhere to DukePay’s development documentation, privacy guidelines and security procedures. A staff member from Treasury and Cash Management will facilitate the implementation of DukePay electronic commerce sites. Departments are responsible for their own transaction management, and the administrative, technical and physical safeguarding of personal information related to purchases of goods and services collected outside of or via DukePay.

6. The department business manager should also give careful thought to the following:

   - Utilizing technical and security best practices in their internal electronic commerce sites
   - Seeking appropriate guidance on banking and financial processes
   - Identifying internal audit implications, sales tax and or UBIT (unrelated business income tax) issues
   - Managing and reporting intellectual property matters
   - Adhering to rules of advertising (most advertising revenue is subject to UBIT). Corporate sponsorships could also constitute advertising and result in unrelated business income, especially if making a comparative statement to its competition
Establishing the appropriate method to report gifts to the University (all gifts must come through Alumni & Development Records).

Adhering to rules for charging/depositing to grant codes

Addressing privacy of users

Addressing legal requirements (e.g. FERPA, HIPAA, GLB Act) to ensure privacy and security of information

Consulting on and receiving approval for the appropriate use of Duke Photography or Duke’s image, logo, or marks.

**SOURCES OF MORE INFORMATION**

E-Commerce @ Duke: finance.duke.edu/banking/ecommerce/
Payment Card Industry Security Standards Council - www.pcisecuritystandards.org/


**UBIT (Unrelated Business Income Tax):** An activity is an unrelated business (and subject to tax at corporate rates) if it meets three requirements: it is a trade or business, it is regularly carried on, and it is not substantially related to the furtherance of the exempt purpose of the organization. There are, however, a number of exclusions and modifications to this general rule. See the Internal Revenue Service: http://www.irs.gov/charities/article/0,,id=96104,00.html

**FERPA (Family Educational Rights and Privacy Act):** A Federal law that protects the privacy of student education records. See http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

**HIPAA (Health Insurance Portability and Accountability Act):** Purpose is to improve the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information. See http://www.hhs.gov/ocr/privacy/

**GLB (Graham-Leach-Bliley Act):** Includes provisions to protect consumers’ personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. See the Federal Trade Commission (www.ftc.gov).