

Electronic Commerce

- Authority** This Guide Memo was approved by the Vice President for Business Affairs and Chief Financial Officer.
- Applicability** This policy applies to all Stanford entities that generate revenue through fundraising or the provision of goods or services.
- Summary** This policy provides guidelines on the use of electronic commerce at Stanford. Section headings are:
1. DEFINITION
 2. PURPOSE
 3. POLICY
 4. IMPLEMENTATION GUIDELINES
 5. SOURCES OF MORE INFORMATION

1. DEFINITION

For purposes of this policy, electronic commerce is defined as the use of electronic ordering and payment mechanisms via an interactive electronic mechanism such as the World Wide Web to effect remote payment for Stanford University goods or services. This policy does not cover business-to-business e-commerce pursuant to which the University purchases goods or services or to electronic ordering and payment mechanisms that are typically used between other businesses or institutions and Stanford University, usually referred to as Electronic Data Interchange (EDI) or Electronic Funds Transfer (EFT).

2. PURPOSE

Electronic commerce provides a convenient way to handle business transactions such as conference registration or the purchase of course materials. However, reasonable steps should be taken to protect the personal information and privacy of purchasers. It is also in the University'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 for electronic commerce.

3. POLICY

- a. **Relation to University Mission** – Any use of electronic commerce at Stanford must be consistent with Guide Memo 15.3, Unrelated Business Activity, http://adminguide.stanford.edu/15_3.pdf, which prohibits the use of Stanford resources for any activity not related to the University's mission.
- b. **Authorized Vendor** – Stanford has contracted with an internet commerce transaction services vendor to handle the authorization and management of electronic orders. This arrangement allows the University to:
 - Consistently require the vendor to take necessary and reasonable steps to ensure that transactions are secure,
 - Assure appropriate integration with University financial systems,
 - Ensure that parties comply with Stanford 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.

Departments wishing to engage in electronic commerce must either use the authorized vendor to provide online order management services or offer evidence to the Controller, or his/her designee, that the selected vendor cannot meet the department's business needs and that an alternative vendor meets University requirements for security and for integrating transaction information into Stanford financial systems. Note that all such agreements should be in accordance with Guide Memo 14, Academic and Business Relationships with Third Parties, <http://adminguide.stanford.edu/14.pdf>.

- c. **Confidentiality of Data** – Departments are responsible for safeguarding the confidentiality of restricted and sensitive data related to purchases of goods or services as stated in Guide Memo 63, Information Security, <http://adminguide.stanford.edu/63.pdf>. Specific eCommerce guidelines are:

- (1) Use secure and/or encrypted connections to the transaction service vendor (such as the one provided to Stanford by its authorized vendor).
- (2) Do not store any restricted electronic payment information (e.g., credit card numbers or PINs) locally, without prior authorization from the risk assessment workgroup designated by eCommerce Strategic Advisory Committee, (eSAC).
- (3) If gathering other information about purchasers, protect this information in a secure manner, restricting access to those who have a valid need to know.

Departments should adhere to Stanford's e-commerce privacy guidelines and security procedures, linking to the guidelines/procedures at each point-of-sale. If a valid business reason dictates departure from privacy guidelines, departments should explicitly advise customers at the point(s) of sale of how their practice departs from University guidelines.

- d. **Advertising Policy** – Departments are responsible for creating the web interface to the vendor's on-line order management system. If the website is in the stanford.edu domain, no third-party advertising is allowed.

4. IMPLEMENTATION GUIDELINES

- a. Stanford eCommerce stores must meet the Payment Card Industry Customer Information Security Program (PCI-CISP) standards.
- b. Additional assistance on setting up and running an electronic commerce store is available on the eCommerce @ Stanford site. Departments should work with representatives of the eCommerce Technical Team, their applications development support team, Controller's Office and Procurement to create their electronic commerce-enabled website.

5. SOURCES OF MORE INFORMATION

- Administrative Guide Memo 14, Academic and Business Relationships with Third Parties, <http://adminguide.stanford.edu/14.pdf>
- Administrative Guide Memo 15.3, Unrelated Business Activity, http://adminguide.stanford.edu/15_3.pdf
- Administrative Guide Memo 63, Information Security, <http://adminguide.stanford.edu/63.pdf>
- eCommerce @ Stanford, <http://ecommerce.stanford.edu/>
- Payment Card Industry - Customer Information Security Program (VISA), http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html
- Information Security Office, <http://security.stanford.edu>
- Additional information security guidelines, procedures, standards, and practices can be found at <http://securecomputing.stanford.edu>