

Credit Card Acceptance and Processing

- 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 accept payments via credit cards or pin-less debit cards.
- Summary** This policy provides guidelines on acceptance and processing of credit cards or pin-less debit cards 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, credit card acceptance and processing is defined as the use of mechanisms such as a point-of-sale terminal or a payment page on a web site to accept credit cards for payment of goods or services sold by a Stanford University entity. The term "credit cards" as used in this policy includes the use of pin-less debit cards bearing a credit card company logo. This policy does not apply to the StanfordCardPlan or to the University's PCard or Travel credit card programs.

2. PURPOSE

Credit cards provide a convenient way to handle business transactions such as conference registration, the purchase of course materials, or the purchase of meals at a campus dining facility. Acceptance of credit cards is subject to the Payment Card Industry's prescriptive requirements for safeguarding cardholder account numbers and other sensitive data. It is also in the University's best interest to facilitate the transfer of credit card transaction data to its financial systems. The purpose of this policy is to establish guidelines for credit card acceptance and processing.

3. POLICY

- a. **Relation to University Mission** – Any use of credit card acceptance and processing methods 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** – Departments must use a Stanford authorized payment application, hosted service provider, or point-of-sale terminal hardware vendor. These are listed at <http://merchantservices.stanford.edu>.
- c. **University Merchant Agreement** – Departments wishing to engage in point-of-sale or internet electronic commerce must be approved by the Controller's Office Credit Card Merchant Services and comply with all terms of the University's Merchant Agreement.
- d. **Confidentiality of Data** – Credit Card Data is classified as Restricted 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 credit card acceptance and processing guidelines are:
 - (1) Use secure and/or encrypted connections to the transaction service vendor (such as the ones provided to Stanford by its authorized vendors).

- (2) Do not store any restricted credit card information (e.g., credit card account numbers or PINs) locally, without prior authorization from the risk assessment workgroup designated by the 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.

e. For departments operating electronic commerce web sites:

- (1) Departments must post a privacy policy on their web site that has been approved by the University Privacy Officer or the Office of the General Counsel. This policy must conform to applicable federal and state laws, as well as the University's privacy policies.
- (2) No third-party advertising is allowed on any web pages which are hosted on the stanford.edu domain, or which use Stanford's name or emblems. Exceptions to this policy may be granted by the Vice President for Business Affairs and CFO. Advertising does not include mentioning the name of third parties which are co-sponsoring events with Stanford.

4. IMPLEMENTATION GUIDELINES

- a. Merchants accepting credit cards are responsible for complying with Payment Card Industry Data Security Standards.
- b. Information about requesting credit card merchant services and assistance on setting up and running an electronic commerce web site is available on the Gateway to Financial Activities web site, <http://fingate.stanford.edu>. Departments should work with representatives of the Controller's Office (Credit Card Merchant Services, Cash Management), IT Services Application Support, and the Procurement Office to establish and manage payment card acceptance and processing.

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>
- Stanford authorized payment applications and service providers, <http://merchantservices.stanford.edu>
- eCommerce @ Stanford, <http://ecommerce.stanford.edu/>
- Payment Card Industry Data Security Standards, <http://www.pcisecuritystandards.org>
- Information Security Office, <http://security.stanford.edu>
- Additional information security guidelines, procedures, standards, and practices can be found at <http://securecomputing.stanford.edu>