3.4.2 CARD AND PAYMENT ACCOUNT ACCEPTANCE AND PROCESSING

This policy provides guidelines on acceptance and processing of credit and debit card, account number, or third party account numbers at Stanford.

Authority:
Approved by the Vice President for Business Affairs & Chief Financial Officer.

Applicability:
Applies to all Stanford entities that accept payments via credit or debit card accounts or financial account numbers or third party account numbers either directly into a Stanford owned merchant account; or indirectly where a third party company accepts card or payment account payments on behalf of the University and then remits payment to a Stanford owned bank account. Section 5 of this policy applies to all third-party vendors or service providers that conduct business at Stanford.

1. Definition

The term "card or payment account" as used in this policy includes the use of credit or debit card accounts or account numbers (such as a bank account) or third party account numbers (such as a PayPal or Google accounts). For purposes of this policy, card or payment account acceptance and processing is defined as using any application or device for accepting a card or payment account as payment for goods or services sold by a Stanford University entity. This policy does not apply to the Stanford Card Plan, Cardinal Dollars or to the University's PCard or Travel credit card programs.

2. Purpose

A card or payment account provides 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. In order to accept card or payment account payments it is the University's best interest that the acceptance and processing is compliant with Payment Card Industry Data Security Standards for safeguarding card numbers, account numbers, and other High Risk Data as listed in Administrative Guide Memo 6.3.1 [1]: Information Security. In addition, funds from payments must be securely transferred to the University's financial systems. This policy is to establish guidelines for card or payment account acceptance and processing.
3. Policy

a. Relation to University Mission
Any use of card or payment account acceptance and processing methods at Stanford must be consistent with Administrative Guide Memo 1.5.3, Unrelated Business Activity, which prohibits the use of Stanford resources for any activity not related to the University's mission.

b. Authorized Vendors and Service Providers
Departments must use a Stanford authorized payment application, payment mechanism, point of sale terminal hardware vendor (if applicable). These are listed at http://treasurer.stanford.edu/merchants/ [2].

A service provider that stores, processes, or transmits cardholder data on behalf of the University must be validated as a Level 1 service provider by a Qualified Security Assessor (QSA) and listed on Visa’s Global Registry of Service Providers. The company listing must be current and the service being provided to the University must match the service listed on Visa’s website.

A company providing a service that can affect the security of an eCommerce transaction (eTransaction) must be validated by a QSA as a service provider and the service being provided to the University must match the services validated as compliant during the QSA assessment.

c. University Card and Payment Account User Agreement
Departments wishing to engage in accepting card or payment accounts for the sale of goods or services must obtain approval from the Office of the Treasurer and comply with all terms of the University's Card and Payment Account User Agreement.

d. Information Security
Card and payment account numbers are classified as High Risk Data. Departments must comply with Administrative Guide Memo 6.3.1: Information Security, and safeguard the confidentiality of High Risk Data related to purchases of goods or services. They may not store any High Risk card or payment account information. They must only use equipment authorized by the Office of the Treasurer to process payment information and are required to use secure and approved, or PCI DSS certified, encrypted connections to transmit payment information.

e. For departments operating electronic commerce websites:
(1) Departments must post a privacy policy on their website that is approved by the University Privacy Officer or the Office of the General Counsel. Vendors and/or Service Providers who independently collect card or third party account information must have privacy and terms of use policies on their websites. These policies must conform to applicable federal and state laws, as well as the University's privacy policies.
(2) Third-party advertising is not 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 that are co-sponsoring events with Stanford.

4. Implementation Guidelines

a. Departments accepting card or payment accounts are responsible for complying with Payment Card Industry Data Security Standards (PCI DSS) and all card brand rules and regulations if applicable, or using
secure standard financial industry practices, if PCI DSS standards are not applicable.

b. Information about requesting a merchant account for payment acceptance is available at the Office of the Treasurer's website [2]. Departments must work with representatives from the Treasurer's Office and the Procurement Office to establish and manage card and payment account acceptance and processing.

5. Third Party Vendors/Service Providers Operating on Stanford's Campus

Third party vendors and service providers operating on Stanford's campus must handle data and other information generated from financial transactions involving the Stanford community ("Data") according to the Third Party Security Requirements listed on the Information Security Office's website [3].

6. Sources of More Information

- Administrative Guide Memo 1.4.1 [4], Academic and Business Relationships with Third Parties
- Administrative Guide Memo 1.5.3 [5], Unrelated Business Activity
- Administrative Guide Memo 6.3.1 [6], Information Security
- Additional information security guidelines, procedures, standards, and practices can be found at http://securecomputing.stanford.edu [9]