UNIVERSITY OF SAN FRANCISCO

Credit Card Acceptance Policy

POLICY CONTENTS

Effective Date: June 21, 2016
Last Updated: June 21, 2016

Responsible University Officer:
Vice President for Business and Finance

Policy Owner:
Associate Vice President for Accounting and Business Services

Policy Contacts:
Desmond Dair

POLICY STATEMENT

Departments authorized to accept credit card payments in connection with the sale of University goods or services must ensure that adequate cardholder data security procedures have been implemented, in accordance with the requirements set forth in this Policy. The Policy conforms to the Payment Card Industry (PCI) Data Security Standards (DSS), which are designed to protect cardholder information from identity theft and other unauthorized uses. Compliance with the Policy is mandatory for both departments and any third parties processing credit card transactions or accessing cardholder data on behalf of the University.

Departments may establish more restrictive procedures than those included in this Policy, if desired.

REASON FOR POLICY

This Policy establishes standards for the processing of credit card payments received by the University in compliance with applicable state and federal laws and industry standards governing such transactions.

WHO SHOULD READ THIS POLICY

Any employee responsible for processing credit card payments received by the University; the member of the Leadership Team, as well as supervisors and Business Managers who supervise an employee with such responsibilities.

POLICY TEXT

Departments interested in accepting credit card payments are required to submit a request to the Office of Accounting and Business Services (ABS) in order to gain access to the University's online credit card payment system. Department employees approved to accept credit card payments, however, must attend training conducted by ABS before access will be granted. See **PCI DSS Training.**

University eCommerce/Online Payment System

The University has adopted CASHNet (aka Transact) as the enterprise-wide solution to manage online credit card payment transactions. Departments proposing to use another vendor must obtain prior approval from the Office of Information Technology Services (ITS) and ABS. See **Authorization**.

PCI Compliance

The Payment Card Industry (PCI) Data Security Standard (DSS) represent a common set of security standards mandated by the payment card industry in order to ensure the safe handling of sensitive cardholder data collected by merchants. The standards are updated periodically by the PCI Security Standards Council, which was created to administer the security requirements on behalf of the industry. The current PCI DSS represents a set of twelve requirements grouped into six areas governing the processing of credit card transactions.
Departments authorized to accept credit card payments must comply with the PCI DSS requirements identified in this Policy as department responsibilities. See **Appendix A**.

Employee Background Checks

New employees must undergo a background check prior to assuming any responsibilities related to the acceptance or processing of credit card payments. If an existing employee is assigned such duties, a background check will be required if one was not performed when the individual was hired. Departments must arrange with Human Resources to schedule a background check, which will be conducted by the University's third-party service provider. See **Background Check Policy**.

Debit Cards

The acceptance and processing of debit card transactions is subject to the same procedures and requirements applicable to credit card payments included in this Policy. Only debit cards with Visa and MasterCard logos will be accepted. Debit card charges are processed as credit card transactions in the payment system.

Donations Made by Credit Card

Donations and contributions paid with credit cards are only processed by the Office of Development, which will send the donor a written acknowledgement confirming the receipt of his or her gift to the University. See **Gift Acceptance Policy**.

Inter-Department Charges

Departments should not accept Purchasing Card payments from another University department, except the University Bookstore and Campus Dining Services, which are managed by outside vendors. The Purchasing Card is intended only for purchasing goods from third-party vendors. Inter-department payments should be processed using a **Request for Funds Transfer** form. See **Purchasing Card Policy**.

PROCEDURES

Authorization
Access
Processing Credit Card Transactions
POS Equipment Authorized for Use
Third-Party Vendors
Security Breach Response
PCI DSS Training
Violations

RELATED INFORMATION

Type	Title
USF	**Background Check Policy**
USF	**Department Cash Handling Policy**
USF	**Gift Acceptance Policy**
USF	**Information Security Policy**
USF	**Physical Inspection for Point of Sale (POS) Terminal—PCI Compliance Standard Operating Procedure (SOP)**
USF	**Purchasing Card Policy**
USF	**Technology Resources Appropriate Use Policy**
External	**Payment Card Industry (PCI) Security Standards Council**

DEFINITIONS

Term	Definition
Business Manager	A University employee, designated by the President, Vice President, Vice Provost, or Dean who is the financial manager for the University account(s) being used for the expense. This may include the President, Vice Presidents, Vice Provosts, or the Deans.
Cardholder Data	Any personally identifiable information associated with a credit (or debit) card, including but not limited to, account number, expiration date, security code, and the name, address, or other identifying information about the cardholder.
CASHNet	The University enterprise solution for the online processing of credit card payments and integration with the University's other enterprise information systems.
PCI Cashier	An employee authorized to enter credit card information into the University's payment system for processing. Such individuals have attended PCI DSS Training for the secure handling of cardholder data and transactions.
Credit Card	A card issued by a commercial bank or financial institution under the Visa or MasterCard brand or by an independent company (e.g., American Express, Discover, etc.) that permits the holder to pay for goods and services by drawing against a line of credit granted by the card issuer.
Debit Card	A card issued by a bank or financial institution under the Visa or MasterCard brand that permits the holder to pay for goods and services by drawing against available funds resident in the payer's checking or savings account at the time of payment. Debit card transactions are processed either online (i.e., PIN debit) or off-line (i.e., signature debit).
FOAPAL (or FOAP)	The acronym representing each element of the University's chart of accounts, including Fund, Organization, Account, Program, Activity, and Location.

ADDITIONAL CONTACTS

Subject	Contact	Phone Number	Email or URL
ABS	Desmond Dair	415-422-6732	**ddair@usfca.edu**
Disbursement Services	Dennis Miller	415-422-2734	**millerd@usfca.edu**
Cashier	*vacant* Opinder	415-422-2579	
ITS, CIO	Bawa	415-422-2787	**osbawa@usfca.edu**
ITS, Information Security	Nicholas Recchia	415-422-2123	**nprecchia@usfca.edu**
OGC	Donna Davis	415-422-6822	**davisdj@usfca.edu**
Payment Requests	Disbursement Services	415-422-2387	**ap@usfca.edu**

PCI DSS Training/iPads	Ivy Efendioglu	415-422-2731	**ivy@usfca.edu**
Tax Compliance	Dominic Daher	415-422-5124	**dldaher@usfca.edu**

FORMS

Form	Use	Location
Acceptable Use Policy (AUP) & Agreement for POS Devices and PCI Network	Used to document employee's agreement to comply with credit card acceptance terms and conditions.	ABS
Credit Card Payment Authorization Form	Used by departments to record cardholder information in connection with mail or telephone transactions.	ABS
Department Deposit Record (DDR)	Used to deliver cash, checks, and credit card slips to the University Cashier for deposit.	ABS
Request for CASHNet e Market Payment Portal	Used by departments to request authority to accept credit card payments.	ABS
Request for Fund Transfer	Used to process inter-departmental payments.	ABS
User Agreement for iPads	Used to rent iPad and related equipment from ABS.	ABS

RESPONSIBILITIES

Department/Business Manager

- Seek ABS approval prior to selecting a third-party vendor application with a credit card payment component.
- Completes **Request for CASHNet eMarket Payment Portal** form to accept online credit card payments.
- Ensures that all employees with credit card processing duties have undergone a background check.
- Ensures that cardholder data is secured and that access is restricted to authorized staff only.
- Delivers completed **Credit Card Payment Authorization Forms** to the University Cashier with the DDR if the department does not have an online payment portal.

- Ensures that employees granted access to the payment system attend annual PCI DSS training.
- Performs periodic equipment inspection and reports suspected or potential security breaches, including equipment tampering, immediately to **infosecurity@usfca.edu**.
- Informs ABS when a PCI Cashier has been transferred or separated from the University.
- Responsible for performing the PCI data security tasks assigned to departments in **Appendix A**.

PCI Cashier

- Securely processes credit cards in the online payment system.
- Attends annual PCI DSS Training.
- Complies with requirements set forth in the **Acceptable Use Policy & Agreement**.
- Performs periodic equipment inspection as required under this Policy.

Accounting and Business Services

- Reviews and approves, as appropriate, department requests to accept credit card transactions, in accordance with this Policy.
- In consultation with the Office of General Counsel, reviews proposed contracts with third-party vendors and service providers to process credit card transactions or access cardholder data.
- Creates and manages online payment pages.
- Authorizes and maintains user access and list of approved users.
- Conducts annual PCI DSS training and executes **Acceptable Use Policy & Agreement** for employees granted access to the payment system.
- Processes **Credit Card Authorization Forms** submitted by departments with the DDR.
- Provides departments with temporary access to iPads and related equipment for events where credit cards will be accepted.
- Assists ITS, as needed, in responding to suspected security breaches reported by PCI Cashiers and other individuals.
- Responsible for performing the PCI data security tasks assigned to ABS in **Appendix A**.

Office of General Counsel

- In consultation with ABS and ITS, reviews proposed contracts with third-party vendors and service providers to process credit card transactions, access cardholder data, or purchase of POS terminals, software applications, and similar technology.

Vice President for Information Technology and Chief Information Officer

- In consultation with ABS, reviews proposed contracts with third-party vendors and service providers to process credit card transactions, access cardholder data, or purchase POS terminals, software applications, and similar technology.
- Installs required security features on POS devices furnished to departments with authorized access to the payment system.
- Enables access to PCI network and maintains list of PCI Cashiers.
- Maintains inventory of POS devices permanently assigned to departments and personnel authorized to use devices.

- Investigates reported security breaches, including equipment tampering and other suspicious activities, affecting cardholder data security.
- Responsible for performing the PCI data security tasks assigned to ITS in **Appendix A**.

Vice President for Business and Finance

- In consultation with ITS and OGC, reviews and approves, as appropriate, proposed contracts with third-party vendors and service providers to process credit card transactions, access cardholder data, or purchase POS terminals, software applications, and similar technology.

President, Vice Presidents, Vice Provosts, and Deans

- Ensures that employees in his or her division with credit card processing responsibilities are in compliance with this Policy.

FREQUENTLY ASKED QUESTIONS

(N/A)

REVISION HISTORY

06/21/2016	First publication of Policy.

APPENDICES

Appendix A	PCI Data Security Standards

PROCEDURES

AUTHORIZATION

Departments must request prior approval from the Associate Vice President for Accounting and Business Services, or his or her designee, in order to accept credit card payments. Departments are not authorized to contract directly with third-party vendor for the processing of credit card transactions or accessing cardholder data.

Proposed contracts for credit card services, the purchase of point-of-sale (POS) terminals, or similar electronic equipment and services require prior approval by both the Vice President for Business and Finance and the Vice President for Information Technology and Chief Information Officer, or their designees. Such contracts must also be reviewed by the Office of General Counsel (OGC).

ACCESS

Departments requesting PCI Cashier access must complete the **Request for CASHNet eMarket Payment Portal** form and submit it to ABS for approval. Request should include the employee's name, University email address, CWID, title, and campus phone.

PCI Network

Users approved by ABS will be added to the PCI network managed by ITS. Such users are required to use a dedicated POS laptop, tablet, or other terminal when processing credit card transaction and must comply with the requirements set forth in the **Acceptable Use Policy & Agreement**.

PCI Cashier Access

Once an approved user completes PCI DSS Training, the user becomes a PCI Cashier and is authorized to process credit card payments on behalf of the University. Access may also include transaction inquiries, voiding and refunding of transactions, and report generation. Both staff and student employees are eligible to become PCI Cashiers.

Reporter Access

Limited access may be provided to users to perform transaction inquiries and generate reports. Reporters do not have access to perform cashiering functions such as entering, voiding and refunding credit card payments.

Access Termination

Department must notify ABS when a user no longer requires access due to change in duties, transfer, or separation from the University.

PROCESSING CREDIT CARD TRANSACTIONS

Credit card payments may be processed for both "cardholder present" and "cardholder not present" transactions, as provided below.

Cardholder Present
Under these circumstances, the cardholder is physically on site to present his or her credit card to department staff for input into the POS terminal. The transaction is completed when the authorization code is received.

If a department is not using a POS terminal, the cardholder's information must be collected using the **Credit Card Payment Authorization Form**. The Form should be correctly signed by the cardholder and attached to the **Department Deposit Record (DDR)** when the department makes its next deposit with the University Cashier. See **Department Cash Handling Policy**.

Credit card payments may only be accepted for the amount of the actual purchase. Cash back and cash advance customer transactions are prohibited.

Cardholder Not Present
When a cardholder is not physically present, the cardholder's data (i.e., name, card number, expiration date, billing address, etc.) would typically be collected online or by telephone.

- **Online Payments** – Customers accessing the on-line payment page must enter their own personal credit card information when making a purchase. Such transactions require no intervention by department staff.

- **Mail and Telephone Payment Requests –** All requests received by mail or telephone to charge a customer's credit card must be processed as follows:

    - For mailed requests, the cardholder's signature and name (legible) must be entered on the department's authorization form used for such requests.

    - The credit card account number and, in most cases, three-digit security code must be provided along with the card expiration date.

    - The correct billing address for the credit card must be provided.

    - Prior to processing, all department authorization forms containing cardholder data must be stored in a safe or locked cabinet or drawer, accessible only by authorized persons, in order to protect cardholder information.

    - Only debit cards with Visa and MasterCard logos will be accepted for mail or phone orders. PCI Cashiers shall ***not*** collect PIN numbers. These will be processed as credit card transactions.

    - The transaction is completed when an authorization code is generated. If a transaction is rejected, the PCI Cashier should contact cardholder.

    - After a transaction has been authorized, only the last four digits of the account number and the authorization code may be retained. All other card information must be redacted or destroyed. Redacting stamps, which can be obtained from ABS, must be used at all times, not black marker pens.

- Departments should only store cardholder data for processing recurring payments. If cardholder data is stored electronically, it must be encrypted with access restricted to authorized persons with user ID and password protection. Hard copies of cardholder data must be stored in a safe or locked cabinet at all times.

- **Email and Fax Payment Requests -** For data security reasons, credit card information should
  never be requested or transmitted via email. Departments may accept credit card payments via fax transmission only if the fax machine is housed in a secure location with restricted access. Departments, however, are prohibited from sending any credit card information via fax or email.

Credit Card Payment Authorization Form
Cardholder data collected by a department for all cardholder present and not present transactions must be entered on the **Credit Card Payment Authorization Form** and submitted to the University Cashier with the DDR.

POS EQUIPMENT AUTHORIZED FOR USE

All POS terminals, laptops, tablets, and readers used for processing credit cards must be configured by ITS to prevent retention of cardholder data. ITS will maintain an inventory of such devices provided to departments for credit card processing. Departments are responsible for safeguarding these devices from any unauthorized use, tampering, destruction, or loss and are subject to periodic audits to ensure that these requirements are satisfied. Terminals should be regularly inspected in accordance with the requirements contained in the **Physical Inspection for Point of Sale (POS) Terminal—PCI Compliance Standard Operating Procedure (SOP)**.

Tablets and Card Readers for CASHNet Mobile

CASHNet includes an app and card reader for the Apple iPad as a mobile solution to securely accept credit card transactions. Both the iPads and associated card readers may be obtained from ABS for temporary use, at no cost to a department. This equipment must be reserved in advance and returned promptly after the conclusion of the event where credit cards are to be processed. To reserve an iPad and card reader, departments must complete and sign the **User Agreement for iPads**. See **Additional Contacts**.

The purchase of all POS equipment used for credit card processing requires prior approval as provided in this Policy. See **Authorization**.
RETURN TO TOP

THIRD-PARTY VENDORS

The University will only contract with third-party vendors that are PCI-complaint. Such contracts must be forwarded to ABS, OGC, and ITS for review and approval. See **Authorization**. If a vendor is approved to process credit card transactions on behalf of the University, the vendor must maintain its PCI DSS certification during the entire period of the contract.

SECURITY BREACH RESPONSE

Employees are required to immediately report known or suspected compromises of University information security, including equipment tampering and other suspicious activities, to **infosecurity@usfca.edu**. The ITS Security Coordinator will inform ABS regarding the security breach and the Department of Public Safety, if it appears that a crime may have been committed. See **Information Security Policy**.

ABS staff will assist the ITS Security Coordinator in the investigation of the incident and in correcting any potential compromises in the security of cardholder data.

PCI DSS TRAINING

Department staff approved to process credit card transactions must attend the PCI DSS training conducted by ABS before receiving access. The training is intended to educate users on processing credit cards and safeguarding cardholder data. Individuals who have completed the training must sign the **Acceptable Use Policy & Agreement**.

PCI Cashiers are also required to attend the PCI DSS Training on an annual basis. If an employee fails to attend the annual training, his or her access to the system will be deactivated. To schedule the PCI DSS Training, see **Additional Contacts.**

VIOLATIONS

A violation of any portion of this Policy may result in the restriction, suspension, or termination of the employee's access to the payment system. The employee may also be subject to disciplinary action, up to and including termination of employment and/or legal action. In addition, an employee may be held personally liable for any financial loss incurred by the University as a result of the employee's failure to comply with the requirements set forth in the Policy.
PCI Data Security Standards.

Appendix A

The table below includes the Data Security Standards published by the PCI Security Standards Council. The standards have been adopted by the University and apply to all departments authorized to accept credit card payments. Some of the requirements have been addressed centrally by the University or its e-commerce vendors. The remaining requirements, however, apply to all departments that process, store, or transmit credit card transactions.

Control Objective	Requirement	Responsibility?		
		Dept.	ITS	ABS
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data.		Yes	
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.	Yes	Yes	Yes
Protect cardholder data	3. Protect stored cardholder data.	Yes	Yes	
	4. Encrypt transmission of cardholder data across open, public networks.		Yes	
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update anti-virus software programs.	Yes	Yes	
	6. Develop and maintain secure systems and applications.		Yes	
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know.	Yes		
	8. Identify and authenticate access to system components.			Yes
	9. Restrict physical access to cardholder data.	Yes		
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data.		Yes	
	11. Regularly test security systems and processes.		Yes	
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.		Yes	