San Francisco State University
Payment Card Policy

Payment Card Industry Data Security Standard (PCI DSS)

Contents

Revisions/Approvals

Ver. #	Changes By	Ver. date	Reason
1.0	J. Green	9/29/2023	Original version

Purpose

This document and additional supporting documents represent San Francisco State University's policy to prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of payment card processing privileges, and fines imposed on and damage to the reputation of the unit and the institution.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express, and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/ organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)

In order to accept payment cards, San Francisco State University must prove and maintain compliance with the PCI DSS. San Francisco State University's Payment Card Policy and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data. This is done in order to reduce the institutional risk associated with the administration of card payments by individual departments and to ensure proper internal control and compliance with the PCI DSS.

Visa Cardholder Information Security Plan (CISP)

Visa Inc. instituted CISP in June 2001. CISP is intended to protect Visa cardholder data wherever it resides, ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into PCI DSS.

MasterCard Site Data Protection Program (SDP)

The SDP Program, with the PCI DSS as its foundation, details the data security and compliance validation requirements in place to protect stored and transmitted MasterCard payment account data.

Scope/Applicability

The San Francisco State University Payment Card Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of San Francisco State University.

Authority

San Francisco State University policies fall within a greater hierarchy of laws, statutes, and regulations. The CSU Board of Trustees has been authorized by the State to govern San Francisco State University. The Board has delegated the authority to manage the San Francisco State University to the President and the president has delegate the authority on these financial matters to the Vice President of Administration and Finance and CFO. As a part of that

management, the Vice President will direct the development and implementation of San Francisco State University's financial policies and procedures.

The following California State University System policies are also included within this authority:
ICSUAM 8000 et sq. - Information Security Policy
ICSUAM 6340 - Credit/Debit Card Payment Policy

Policy

It is the policy of San Francisco State University to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Office of the Controller and the Bursar. San Francisco State University requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this policy document, the San Francisco State University Payment Card Procedures, and other supporting documents.

SF State entities (also known as university merchants) accepting payment cards online, in person, or over the phone are required to obtain pre-approval by the Bursar's Office, UCorp, Procurement, and the Information Security Office before accepting transactions. All merchant accounts for processing payment cards must be registered with SF State Financial Services, Bursar's Office, or UCorp. This ensures all requirements for card processing systems, including but not limited to, establishing a new merchant account, setting up equipment, and processing transactions, etc., are compliant with current PCI DSS and the University's policy and procedures (https://sfsu.app.box.com/s/pykq5b2yvujihwznsalzihln0ej6rt4s). Also, this will ensure that all depository requirements and interfaces are satisfactorily met.

This policy may be updated from time to time as requirements change. Failure to follow the requirements of the agreement may result in the revocation of your ability to accept card payments.

All persons in positions that store, process, transmit, have access to, or affect the security of payment card data will complete PCI DSS training upon hire and at least annually thereafter. These persons will also acknowledge, in writing or electronically, that they have read, understand and will comply with these policies and procedures. Merchants are responsible for notifying the Bursar's Office for any staff required to complete the PCI DSS security training or whenever anyone with access to payment card systems is terminated, transferred, or whose job function no longer requires such access. This includes any entity that utilizes any part of the University network infrastructure for payment card transaction services.

Entities must accept only payment cards authorized by the Office of the Controller and the Bursar and agree to operate in accordance with the contract(s) San Francisco State University or it's University Corporation (501c3) holds with its Service Provider(s) and the Card Brands. This ensures all transactions comply with the PCI DSS, Federal Regulations, National Automated Clearing House Association (NACHA) rules, service provider contracts, and San Francisco State University policies regarding security and privacy that pertain to electronic transactions.

Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Data that is not absolutely necessary in order to conduct business will not be retained in any format. All data will be treated as confidential
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention
- Physical access to data records is restricted to staff with a need to know

Cardholder data (CHD) received via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. Follow approved departmental procedures for the appropriate method of responding to and securely destroying the cardholder data.

SF State will maintain a PCI DSS Council Charter that outlines roles and responsibilities for campus stakeholders to maintain PCI DSS program compliance.

University merchants must use the Technology Acquisition Review (TAR) to obtain security and accessibility reviews and approvals for all payment card equipment acquisitions. The Bursar's Office or UCorp approval is also required and should be contacted prior to the submitted TAR. Devices that capture payment card data via direct physical interaction with the card should be physically secured and protected from tampering and substitution. This includes training personnel to be aware of suspicious activity and the periodic inspections of Point of Sale (POS) devices for tampering. User access to areas that store, process, or transmit cardholder data should be restricted based on individual job function.

To minimize payment card fraud, all public facing websites must utilize enhanced authorization elements (e.g., CAPTCHA, CCV, Address Verification). The implementation of this requirement may vary by application but must be appropriate for the solution and approved by the PCI Council Charter. Merchant is responsible for making sure the Service Providers are compliant.

All payments received must be deposited into an approved San Francisco State University's Bank Account. The type and nature of the electronic transaction (e.g., ACH, Credit Card, Point of Purchase, wire, etc.) will dictate where the transaction will be deposited. Accounting entries to record the receipt of the payment will be linked directly into the institution's Common Financial System (CFS) whenever possible, to ensure timely recording of transactions and expedite the prompt reconcilement of general ledger and bank accounts.

Procedures and Other Supporting Documents

- San Francisco State University - PCI Administration and Department Payment Card Procedures
- San Francisco State University - Appendix 1 - PCI Payment Card Security Incident Response Plan
- San Francisco State University - Appendix 2 - PCI Application for New Payment Card Merchants
- San Francisco State University - Appendix 3 - PCI Annual Merchant Survey
- San Francisco State University - Appendix 4 - PCI Payment Card Best Practices

Additional Resources

SF State Bursar's Office
SF State Confidential Data Handling
Supporting PCI DSS Documents
Red Flag

Interpretations

The authority to interpret this policy rests with the Office of the President and the PCI DSS Council Charter.

Exclusions

Enter exclusions here.

Glossary

Term	Definition
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Cardholder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Cardholder Name	The name of the Cardholder to whom the card has been issued.
CAV2, CVC2, CID, or CVV2 data	The three or four -digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices, (Before disposal or repurposing, computer drives should be sanitized in accordance with the (Institution's) Electronic Data Disposal Policy). The approved disposal methods are: • Cross-cut shredding, Incineration, Approved shredding or disposal service
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
Merchant	Any department or unit (can be a group of departments or a subset of a department) which has been approved by SF State to accept payment cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions.
Payment Card Industry Data Security Standard (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: Visa, MasterCard, American Express, Discover, JCB

PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account and includes a check digit as an authentication device.
Sensitive Authentication Data	Additional Elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Service Code	The service code that permits where the card is used and for what.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).