User Guidelines for Collecting and Processing Credit Card Information	Guidelines No.	ITS-1025-G	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	9-19-12	Revised:	
				Page 1 of 15

Table of Contents

1 Purpose....2
2 Entities Affected by Guidelines....2
3 Definitions....2
4 Guidelines....4
4.1 Controller's Office Approval Required....4
4.2 Personnel Responsibilities....4
4.2.1 Credit Card Handling Department or UAS Administrator....4
4.2.2 Credit Card Processor....5
4.3 Accepting Payment When Cardholder Is Present....5
4.4 Card Won't Read When Swiped....6
4.5 Accepting Payment When Cardholder Is Not Present....6
4.6 Suspicious Activity....7
4.7 Authorization....7
4.8 Refund of a Credit Card Purchase....7
4.9 Chargebacks....8
4.10 Monitoring Transactions....8
4.10.1 Pinpoint Areas with High Key-Entry Rates....8
4.10.2 Measure "Copy Request" Volume....8
4.10.3 Fraudulent Transactions....8
4.11 Steps to Reduce Disputes....9
4.11.1 Name on Customer's Bills....9
4.11.2 Legible Business Name on Receipts....9
4.11.3 Merchandise....9
4.12 Processing....9
4.13 Data Transmission....9
4.14 Data Storage....10
4.15 Prohibited Practices....10
4.16 Equipment....11
4.16.1 Imprint Machines....11
4.16.2 Terminals and Computers....11
4.17 Restrict Physical Access....11
4.18 Retention/Destruction....12
4.19 Security Breach Response Plan....12
4.19.1 Immediately Contain and Limit Exposure....12
4.19.2 Alert All Necessary Parties....12
5 Contacts....12
6 Additional Resources....13
7 Applicable Federal and State Laws and Regulations....13
8 Related Documents....14

1 Purpose

The Payment Card Industry Data Security Standard (PCI DSS), a set of comprehensive requirements for enhancing payment card data security, was developed in 2004 by the founding payment brands of the PCI Security Standards Council, which included American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International. The purpose was to facilitate the broad adoption of consistent data security measures on a global basis. Subsequent revisions have been released that enhanced clarity, improved flexibility and addressed evolving risks and threats. One of these revisions, Version 1.2 released on October 1, 2009, recognized that since universities collect credit card information and process credit card payments, there was a contractual obligation for them to adhere to the PCI DSS, as well as credit card association rules and regulations.

The use of credit cards reduces cash handling on campus, funds are deposited faster, and it greatly enhances the University's and University Auxiliary Services' (UAS) ability to serve its customers. These guidelines set forth the requirements for processing charges on credit cards to protect against the exposure and possible theft of account and personal cardholder information, suggestions for monitoring transactions, steps to take to reduce disputes, and guidelines for responding to a security breach.

Failure to comply with Payment Card Industry rules may result in financial loss, fines, suspension of credit card processing privileges, or damages to the reputation of the University.

2 Entities Affected by Guidelines

These guidelines apply to any official or administrator with responsibilities for managing University credit card transactions and those employees who are entrusted with storing, processing, transmitting, or handling cardholder information in a physical or electronic format.

These guidelines apply to all University Auxiliary Services (UAS) with responsibilities for managing credit card transactions and those auxiliary employees who are entrusted with storing, processing, transmitting, or handling cardholder information in a physical or electronic format.

In addition, all network components involved in processing payment card data are governed by PCI DSS. This includes, but is not limited to, servers, computers, workstations and point of sale terminals that process, transmit or store credit card information.

3 Definitions

a) Acquirer: Also referred to as "acquiring bank" or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

b) Address Verification Service (AVS): AVS allows merchants that accept card-not-present transactions to compare the billing address given by a customer with the billing address on the Issuer's master file before shipping an order. AVS helps merchants minimize the risk of accepting fraudulent transactions in a card-not-present environment by indicating the result of the address comparison.

c) Authorization: The process by which an Issuer approves or declines a card purchase. Authorization occurs automatically when you swipe the magnetic stripe of a payment card through a card reader.

d) Card Expiration Date: The date after which a bankcard is no longer valid. The date is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid. Also known as a "Good Thru Date."

e) Cardholder: Non-consumer or consumer customer to whom a payment card is issued or any individual authorized to use the payment card.

f) Cardholder Data: Any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card.

g) Chargeback: A process that is initiated by the cardholder who may contact credit card issuing bank regarding an inconsistency in the statement. Issuing bank will credit back to the cardholder then charge a fee to the merchant.

h) Code 10 Authorization: When used during a call to the issuer's Authorization Center in the customer's presence, a Code 10 authorization request alerts the card issuer to suspicious activity without alerting the customer.

i) Copy Request: A "copy request" occurs when a customer's card issuer asks the merchant for a copy of a transaction receipt and any additional information that can be provided on a particular charge. This request is most often initiated by the cardholder themselves and generally results from some confusion over the charge that has appeared on their credit card statement.

j) Floor Limit: The maximum amount the merchant can charge to the buyer's card without getting authorization which is typically specified in Merchant Agreements. Floor limits are zero for all card-not-present transactions.

k) Issuer: Also referred to a "issuing bank" or "issuing financial institution." Entity that issues payment cards directly to consumers and non-consumers.

l) Magnetic Stripe Data: Also referred to as "track data." Data encoded in the magnetic stripe or chip used for authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

m) Merchant: A department of the University that has been approved to accept credit card payments under the University Merchant Agreement. The term "merchant" also includes the staff and faculty in the particular department or office.

n) Merchant Bank: A financial institution that enters into agreements with merchants to accept credit cards as payment for goods and services; also called acquirers or acquiring banks.

o) Merchant Card Processor: Bank, Internet service provider, or other firm that provides credit card and electronic commerce transactions but may or may not provide merchant accounts.

p) Payment Card Industry Data Security Standard (PCI DSS): A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It was designed to and includes detailed requirements to minimize the chance of card member data compromise and the effects if a compromise does occur.

q) Personal Identification Number (PIN): Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system.

r) PIN Verification Value (PVV): Discretionary value encoded in magnetic stripe of payment card.

s) Primary Account Number (PAN): Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

t) Rebuttal: A merchant's written reply to a chargeback.

u) Sensitive Areas: Any data center, server room, or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.

v) Sensitive Authentication Data: Security-related information (card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

4 Guidelines

These guidelines are not a complete list of PCI DSS requirements but represent those conditions most likely to occur in a University environment. Any department or UAS entity that accepts credit cards should process transactions in accordance with these guidelines and should also be aware of and follow the rules of the acquirer and the PCI DSS.

4.1 Controller's Office Approval Required

The establishment of control measures for credit card transactions is necessary to maintain proper security over credit cardholder information. The University Controller must approve any department that wants to process, transmit, or handle cardholder information.

4.2 Personnel Responsibilities

4.2.1 Credit Card Handling Department or UAS Administrator

The Credit Card Handling Department or UAS Administrator is responsible for:

- Receiving approval from the University Controller before entering into any contracts or purchases of software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, point-of-sale device) or the number of projected credit card transactions.
- Receiving approval of ITS prior to implementation of any technology, including changes, affecting transactions processing associated with the merchant account.
- Ensuring compliance with Payment Card Industry Data Security Standards, the acquirer, and CSU policies and CSULA standards and guidelines.

- Ensuring all personnel involved in credit card handling receive basic as well as ongoing credit card security training appropriate to their duties.
- Establishing appropriate segregation of duties between credit card processing, the processing of refunds, and the reconciliation function.
- Establishing departmental procedures for safeguarding cardholder information and secure storage of data.
- Ensuring that HRM has performed applicable background checks on potential employees who will have access to systems, networks, or cardholder data as required by PCI DSS. Note: If employees have access to one card number at a time to facilitate a transaction, such as store cashiers, background checks are not required by PCI DSS.
- Restricting access to credit card data and processing to appropriate and authorized personnel and maintaining a list of these employees. Access to computing resources and cardholder data should be limited to only those individuals whose job requires such access.
- Immediately conducting an investigation and notifying the University Controller if a security breach occurs.
- Not using any credit card terminal other than the one designated for and assigned with the merchant identification number for the department.

4.2.2 Credit Card Processor

The credit card processor is responsible for:

- Following departmental procedures for processing, transmitting, or handling cardholder information.
- Reviewing each transaction receipt for accuracy and completeness.
- Ensuring the transaction receipt is readable by changing printer ribbon and paper when needed.
- Giving the cardholder the customer copy of the transaction receipt and keeping the original signed copy.
- Not accepting a transaction if it has been declined.
- Not disclosing or acquiring any information concerning a cardholder's account without the cardholder's consent.
- Resolving disputes timely and efficiently.
- Requesting a Code 10 authorization when there is anything suspicious about a card or a cardholder at any time during a transaction.
- Immediately deleting unencrypted e-mails containing credit card information and notifying the customer that they should not send their credit card information in an unencrypted e-mail.

4.3 Accepting Payment When Cardholder Is Present

This is a payment condition where the payer is physically on site with his/her credit card available for "swiping" through the credit card terminal. The "Cardholder Is Present" model is beneficial since it gives rise to the lowest discount rate from the Merchant Card Processor on the presumption that there will be lower rates of fraud and fewer chargebacks.

In this situation the credit card processor should:

- Ask for identification at the point of sale to verify that the card member is using the card.
- Swipe the card to request the transaction authorization. Hold the card through the entire transaction.

- While the transaction is being processed, check the card's features and security elements to make sure the card is valid and has not been altered in any way.
- Obtain authorization and get the cardholder signature on the transaction receipt.
- If fraud is suspected a Code 10 call should be made.
- Compare the name, number, and signature on the card to those on the transaction receipt.
- Most point-of-sale terminals allow merchants to verify that the account number embossed on the front of the card is the same as the account number encoded on the card's magnetic stripe. If available, match the embossed number on the card to the four digits of the account number displayed on the terminal.
- Check the authenticity of the signature by comparing the signature on the receipt to the signature on the back of the credit card. If the credit card has not been signed then, and only then, ask to see some form of official government identification such as a driver's license or passport. Ask the customer to sign the card in full view and then check the signature to the identification. If the receipt and card do not match, the transaction should not be completed.

4.4 Card Won't Read When Swiped

In some instances, when a card is swiped, the terminal will not be able to read the magnetic stripe or perform an authorization. When this occurs, it usually means one of three things:

- The terminals magnetic stripe reader is not working properly.
- The card is not being swiped through the reader correctly.
- The magnetic stripe on the card has been damaged or demagnetized. Damage to the card may happen accidentally, but it may also be a sign that the card is counterfeit or has been altered.

If a card won't read when swiped, the credit card processor should:

- Check the terminal to make sure that it is working properly and that the card is being swiped correctly.
- If the terminal is okay, take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way.
- If the problem appears to be with the magnetic stripe, follow department procedures.
- For key-entered or voice-authorized transactions, make an imprint of the front of the card. The imprint proves the card was present at the point-of-sale and protects the merchant from potential chargebacks if the transaction turns out to be fraudulent.

4.5 Accepting Payment When Cardholder Is Not Present

This is a payment condition where the payer is not physically on site with his/her credit card and the cardholder data has been collected through the mail, by telephone, or by Web site. Information provided in this manner is generally documented in hard copy. This transaction is completed when the University or UAS presents the data to the Merchant Card processor which obtains an approval or rejection message from the payer's credit card issuer. This payment model is efficient but it does give rise to a higher discount rate from the Merchant Card Processor on the presumption that there will be higher rates of fraud and more chargebacks. In most cases, the merchant site accepting payments in the "Cardholder Is Not Present" model typically must absorb any and all losses that arise from fraud or customer initiated chargebacks.

In this situation the credit card processor should:

- Obtain cardholder name, billing address, shipping address (if different from billing address and if applicable), account number, and credit card expiration date.
- Verify the customer's billing address either electronically (by entering the zip code in the point-of-sale device) or by calling the credit card automated phone system (Address Verification Service).
- Request the Security Code (the three-digit code on the back of the card in the signature panel) and validate the code at the time of authorization either electronically (through the point-of-sale device) or by calling the credit card automated phone system. This code should be destroyed once validated; it should not be stored physically or electronically.

4.6 Suspicious Activity

If the card member or card sale is suspicious, a credit card processor should call the card issuer's Authorization Center and request a Code 10 authorization. A Code 10 authorization request alerts the card issuer to suspicious activity without alerting the customer.

4.7 Authorization

Authorization should be seen as an indication that account funds are available and a card has not been reported as lost or stolen. It is not proof that the true cardholder or a valid credit card is involved in a transaction.

A card acceptor must obtain an authorization from the issuer before completing the transaction in the following instances:

- The transaction amount exceeds the card acceptor's floor limit or the floor limit applicable to the transaction.
- The card is expired or not yet valid.
- The card is not signed.
- The card acceptor wishes to delay presenting the transaction record.
- The transaction receipt cannot be imprinted although the card is present.
- The card acceptor's data processing equipment is unable to read the magnetic stripe or the chip (if one is present) on the card.
- The account number is listed on the Electronic Warning Bulletin or regional Warning Notice. The card acceptor must retain the card by reasonable and peaceful means and notify the Authorization Center for further instructions.
- The transaction is a recurring payment and a previous authorization request was declined.
- The card acceptor is suspicious of the transaction for any reason.

4.8 Refund of a Credit Card Purchase

All refunds of goods and services paid for by credit card shall be made by check.

- Department personnel shall sign each check.
- The amount of the check may not exceed the amount of the original transaction as reflected on the sales draft.
- Specific instructions for refund processing are included in the user manual provided by the acquirer.

4.9 Chargebacks

Credit card returns, also known as chargebacks, are the consequence of:

- Customer disputes
- Fraud
- Processing errors
- Authorization issues
- Non-fulfillment of copy requests (only if fraud or illegible)

The merchant will be notified that cardholders' (payer's) bank intends to process a chargeback prior to the actual debit transaction. This "courtesy" is extended to all merchants to permit the merchant to "dispute" the chargeback, so these notifications should be researched and responded to upon receipt. The merchant is responsible to provide the bank with written proof that the transaction was authorized by the customer. Rebuttals must be completed within the number of days indicated on the chargeback notification.

Chargebacks are debited by the Merchant Card processor to the merchant card account. The chargeback will identify the Merchant ID (with translates to a specific campus department) that accepted the payment and that Merchant ID will be debited for the returned item.

4.10 Monitoring Transactions

Credit card transactions should be monitored to ensure transactions are processed efficiently and effectively and to identify opportunities for improvement.

4.10.1 Pinpoint Areas with High Key-Entry Rates

Calculate the percentage of key-entered transactions compared to total transactions to pinpoint which areas or sales associates have high key-entry rates since key-entry is prone to more errors. Merchants are encouraged to monitor their key-entry rates on a monthly basis. The key-entry rates per terminal or sales associate should be less than 1%.

To obtain the percentage of key-entered transactions for a particular terminal, divide the total number of key-entered transactions by the total number of sales. Exclude from both totals any mail or telephone orders that may have been made at the terminal. Perform the above calculation for each terminal, and for each sales shift to determine the key-entry rate per sales associate.

4.10.2 Measure "Copy Request" Volume

The monthly copy request volume should not exceed 0.16 percent of total sales. To measure this volume, divide the number of copy requests received by total transactions minus returns and adjustments. If the ratio exceeds 0.16 percent, point-of-sale and other business procedures should be reviewed.

4.10.3 Fraudulent Transactions

If a high volume of code 81 (Fraudulent Transaction – Card-Present Environment) chargebacks are being experienced, it should be investigated by the department administrator. Sales receipts related to the chargebacks may need to be examined to determine which terminals and sales staff were involved in these transactions.

4.11 Steps to Reduce Disputes

Steps should be taken to reduce the number of disputes that can arise.

4.11.1 Name on Customer's Bills

Make sure customers can recognize the department name on their bills. Cardholders must be able to look at their statements and recognize transactions that occurred at the department.

4.11.2 Legible Business Name on Receipts

Make sure the department's name is accurately and legibly printed on transaction receipts. The location, size, or color of this information should not interfere with transaction detail. Any department logos or marketing messages on receipts should be positioned away from transaction information.

4.11.3 Merchandise

Ensure that descriptions of merchandise or services shown in catalogs, on Internet screens and sales receipts, or used in telephone order-taking scripts are accurate, complete, and not unintentionally misleading.

Regularly review shipping and handling processes to ensure that orders are being filled accurately.

4.12 Processing

Time limits are set for depositing transactions to ensure timely processing and billing to cardholders. When transactions are held beyond the period defined in the merchant agreement (usually one to five days), money may be lost, customer service may be affected (cardholders expect to see transaction on their statements within the same or next monthly cycle), and a chargeback may be incurred.

On a daily basis, the department must balance transactions and settle their sales electronically to the merchant services provider. The department will complete and send the credit/debit card transmittal form to the University Controller so that the sales revenue can be recorded in the University Accounting System. Transmittal forms summarizing the settled sales should be sent to the University Controller by fax or e-mail no later than noon on the day following settlement.

The University Controller will compare the sales amount per the transmittal to the records at the card processor and will immediately inform the department of discrepancies. All discrepancies should be resolved within 24 hours so that sales can be posted to the departmental account in the CSULA Accounting System on a timely basis.

When the University Controller receives chargeback inquiries from the credit card companies, the applicable department will be contacted to provide the necessary information about the sales transaction in question.

4.13 Data Transmission

Credit card numbers must be transmitted in a secure manner, such as by encrypted e-mail, secured fax, through campus mail using sealed envelopes, or any other secured transmission method. Do not use wireless personal computers for processing credit card data unless approved in writing by ITS.

4.14 Data Storage

Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants. Cardholder data should only be stored if there is a business need justified by the department. The following table summarizes data storage requirements.

Data Storage Summary			
	Data Element	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name[1]	Yes	Yes[1]
	Service Code[1]	Yes	Yes[1]
	Expiration Date[1]	Yes	Yes[1]
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	No	N/A
	CAV2/CVC2/CVV2/CID[4]	No	N/A
	PIN/PIN Block	No	N/A

[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

[4] A Card Verification Value code, CVV, (CVV2 for Visa, CVC2 for MasterCard and CID for AMEX) is the three or four digit number located either on the front or back of a credit or debit card.

Excerpted from PCI Security Standards Council "PCI Data Storage Do's and Don'ts"

- Do not store credit card information in a customer database or electronic spreadsheet.
- If paper records containing credit card numbers are stored, all but the last four digits should be redacted within 60 days, or as soon as refunds or disputes are no longer likely, but no more than 180 days.
- Paper records must be stored in a locked room, cabinet, safe or drawer, to which only authorized employees are permitted access.
- Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as personal computers, laptops, or smart phones.

4.15 Prohibited Practices

Prohibited practices, include among others:

- A merchant must not engage in any acceptance practice that discriminates against or discourages the use of a card in favor of any other acceptance brand.
- MasterCard/Visa regulations prohibit assigning a minimum or maximum purchase amount or adding a surcharge to credit card transactions.

- MasterCard/Visa regulations prohibit listing the cardholder's personal information on the credit card draft/ticket. Such information includes, but is not limited to, telephone number, driver's license, or Social Security number.
- A merchant must not sell, purchase, provide, exchange or in any manner disclose account number information to anyone other than its acquirer or in response to a legal request. This prohibition applies to all media obtained as a result of a credit card transaction.

4.16 Equipment

4.16.1 Imprint Machines

Use of imprint machines to process credit card payments is strongly discouraged, as they display the full 16-digit credit card number and expiration date on the merchant and customer copies. If imprint machines must be used, the merchant must take all precautions necessary to ensure the hard copy is immediately filed in a secure location and is not easily accessible by unauthorized personnel or patrons.

4.16.2 Terminals and Computers

- Do not have terminals print out personally identifiable payment card data; printouts should be truncated or masked with only the last 4 digits of the credit card information disclosed as recommended by major credit cards.
- It is acceptable for point-of-sale devices to store the sensitive cardholder data on their device until the transaction is settled; once settlement occurs, no information should be stored electronically.
- All point-of-sale terminals must be PCI DSS compliant.

4.17 Restrict Physical Access

Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

Controls to be considered include, among others:

- Using video cameras or other access control mechanisms to monitor individual access to sensitive areas.
- Locating servers or other payment card system storage devices inside of a locked, fully-secured and access-controlled room.
- Restricting physical access to publicly accessible network jacks.
- Restricting physical access to wireless access points, gateways, and handheld devices.
- Making sure all visitors are authorized and easily identifiable (e.g., badge or access device) before entering areas where cardholder data is processed or maintained.
- Establishing visitor sign-in logs, escorts and other means to maintain a physical audit trail of visitor activity and to restrict access to documents, servers, computers, and storage media.
- Ensuring management approves any and all media that is moved from a secure area.
- Conducting media inventories at least annually.
- Physically securing and maintaining strict control over all media including internal or external distribution.

4.18 Retention/Destruction

Credit card numbers with cardholder name or expiration date and/or card verification code are classified as Level 1 Confidential Data and should be retained according to CSU Executive Order 1031.

4.19 Security Breach Response Plan

In the event of a breach in credit card data security the following steps should be taken:

4.19.1 Immediately Contain and Limit Exposure

To prevent any further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of accounts or account information within 24 hours of the compromise. Failure to comply with security procedures and rectify the violation may result in heavy fines imposed by the credit card companies.

- Do not access or alter compromised systems (e.g., do not log on or change passwords).
- Do not turn off the compromised machine. Instead, isolate compromised systems from the network by unplugging their cables.
- Preserve logs and electronic evidence.
- Log all actions taken.
- If using a wireless network, change the service set identifier or network name on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
- Be on high alert and monitor all systems with cardholder data.
- Provide the University Controller with a report identifying the account information at risk and the source and timeframe of the compromise.

4.19.2 Alert All Necessary Parties

The merchant department should immediately alert all of the following in this sequence:

- Director of IT Security and Compliance - who may activate the Campus Security Incident Response Team (CSIRT)
- University Controller
- Other entities as identified in the Merchant Bank Agreement.

5 Contacts

a. For questions regarding specific department procedures, contact the department administrator.

b. Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

6 Additional Resources

Resource	Description
Payment Card Industry Security Standards Council	**The PCI Security Standards Council** (the "Council") provides a variety of tools, questionnaires, guidance, FAQs, training resources and other materials and information to assist organizations seeking to achieve compliance with its standards (the "Standards"). Access to the PCI Quick Reference Guide and the PCI Best Practices for Merchants are available at: https://www.pcisecuritystandards.org/index.shtml
California Office of Information Security	**The California Office of Information Security** provides PCI DSS information, guidance, and risk assessment tools that are specific to merchants processing credit card transactions within the State of California. http://www.cio.ca.gov/OIS/Government/risk/toolkit.asp

7 Applicable Federal and State Laws and Regulations

Federal	Title
Fair Credit Reporting Act (FCRA)	**Fair Credit Reporting Act (FCRA), U.S. Code, Title 15 § 1681 et seq.** For the complete text as amended October 2001, visit: http://www.ftc.gov/os/statutes/fcra.hem This is the federal law that protects consumer credit and credit reporting.
Gramm-Leach-Bliley Act 15 USC, Subchapter 1, Sec. 6801-6809	**Gramm Leach Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
State	**Title**
SB 1386	**California Personal Information Privacy Act, SB 1386** http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.

California Civil Code Section 1747.08	**California Civil Code, Section 1747.08** **Limits on Collection of Personal Information when Accepting Payment by Credit Card** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that protects personal identification information in credit card transactions.
California Civil Code Section 1747.09	**California Civil Code – Section 1747.09 Truncation of Credit Card Numbers** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that specifies restrictions for printing more than the last five digits of the credit or debit card account number or the expiration date of the card. [Note: California allows for the display of the last five digits, PCI DSS allows for the display of the first six and last four digits, and major credit cards specify only displaying the last four digits. These guidelines specify the display of only the last four digits.]
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Section 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
California Civil Code Sections 1798.80-1798.81	**California Civil Code – Section 1798.80 – 1798.81 Destruction of Customer Records** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that identifies steps to be taken in the destruction of customer's records.

8 Related Documents

ID/Control #	Title
ITS-2009-S *Pending*	**Credit Card Merchant Requirements and Responsibilities** http://www.calstatela.edu/its/itsecurity/guidelines This standard defines Payment Card Industry Data Security Standard (PCI DSS) requirements to secure against accidental loss or disclosure and ensure that all transactions are in compliance with all credit card association rules and regulations.
CSULA Gramm-Leach-Bliley Information Security Program	**Gramm-Leach-Bliley Information Security Program for CSULA** http://www.calstatela.edu/its/itsecurity/programs/glba.php This document is the Gramm-Leach-Bliley Information Security Plan for CSULA and serves as a guide for how information security is to be maintained at the campus.

ID/Control #	Title
CSU Executive Order 1031	**System-wide Records/Information Retention and Disposition Schedules Implementation** http://www.calstate.edu/EO/EO-1031.html http://www.calstate.edu/recordsretention This Executive Order provides for the implementation of the California State University (CSU) System-wide Records/Information Retention Schedules.
PCI Security Standards Council	**PCI SSC Self-Assessment Questionnaire (SAQ)** https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#instructions This website provides instructions for completing the Self-Assessment Questionnaire.
PCI Security Standards Council	**Merchant & Service Providers Resource Center** https://www.pcisecuritystandards.org/about/resources.shtml This website provides resources for merchants and service providers.
Visa	**Visa Merchants Card Management Guide** http://usa.visa.com/download/merchants/chargeback-management-guidelines-for-visa-merchants.pdf This is a comprehensive manual for all businesses that accept Visa transactions.
MasterCard	**MasterCard** http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf This is a comprehensive manual for all businesses that accept MasterCard transactions.
American Express	**American Express** https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=merchantPolicy&inav=merch_gs_mechpolicy This is a comprehensive manual for all businesses that accept American Express transactions. A merchant account number is required to access the manual.
Discover	**Discover Financial Services** www.discovernetwork.com/resources/data/data_security.html This is the Discover website.