UCR Cashiering & Payment Card Services

TERMINAL CONTROL MEASURES

Instructions: Upon completion, please sign and return to cashandmerchant@ucr.edu when requesting a stand-alone dial up terminal.

The University of California Office of the President mandates that all University of California campuses comply with the Payment Card Industry Security Council's Payment Card Industry Data Security Standard (PCI DSS). (The Security Council has representatives from the five major card brands: Visa, MC, Amex, Discover & JCB.)

A security breach and subsequent compromise of payment card data has far reaching consequences for affected organizations, including:

- ***Regulatory notification requirements***
- ***Loss of reputation***
- ***Loss of customers***
- ***Potential financial liabilities (for example, regulatory and other large fines and fees)***
- ***Litigation***

******In this document "Media" refers to all paper and electronic media containing cardholder data (credit card number, expiration date, card verification codes. ******

Accepting payment cards is a departmental privilege. Departments processing payment cards must abide to the following standards regarding the acceptance and storage of cardholder data. All personnel in the payment card processing environment must read and understand the requirements of the Terminal Control Measures.

All UCR merchants/departments must abide by the following guidelines:

- Departments must not store cardholder data on computers (spreadsheets, etc.) and credit card information (credit card number, expiration date, card verification codes, etc.) must not be transmitted via email. If payments are accepted in-person at a remote location, terminals must be monitored and tracked at all times.

- Strict control must be maintained over the internal or external distribution of any kind of media.

- Media must be classified so that the sensitivity can be determined.

- Media sent or transported must be secured by a courier and accurately tracked.

- Logs must be maintained to track all media that is moved from a secured area.

- Management's approval must be obtained prior to moving media, especially when media is distributed to individuals.

- Each department must designate an individual who holds the primary authority and responsibility for payment card processing.

- Pay the costs associated with payment card processing (bank and interchange fees, equipment fees, if applicable, and other fees as deemed appropriate).

- Comply with all PCI DSS guidelines, UCOP's Business & Finance Bulletin 49 (BUS-49), *Policy for Cash and Cash Equivalents Received*, and UCR's policies and procedures for payment card acceptance and security (200-17).

- Validate PCI compliance annually, which includes the completion of the appropriate Self-Assessment Questionnaire (SAQ) and associated processes, if applicable, as required by the University's acquiring bank and credit card associations.

- Require all those involved with merchant processes, either directly or as a supervisor, to participate in Security Awareness Education (SAE) training annually and upon hire.

- Notify the Campus Credit Card Coordinator (Director of Student Business Services/Cashiers) when a program ends or when changes take place, if applicable.

- Return equipment at the conclusion of a program, if applicable. For inventory purposes.

- Respond to chargeback notifications and credit card company inquiries in a timely manner (within 15 days).

- Ensure that cardholder data is not transmitted or obtained via email or stored electronically in any database, application or system.

- Maintain the physical protection of departmental credit card receipts and the secure destruction of payment card receipts and cardholder data once a program has ended and all payments have been reconciled (no longer than twenty four months maximum, and no less than 12 months minimum).

- Provide full cooperation with the University's Campus Credit Card Coordinator and/or authorized third-party assessors whenever necessary.

- Authorize and complete deposit settlement daily. (Strongly recommend setting up auto-settle)

- One DAF per day per Merchant ID must be created daily for each day there is credit card activity.

Physical Access Control

- Credit card terminals must be kept in a secure location with limited physical access.

- Terminals need to be inspected daily for tampering and a log maintained documenting the review.

- Cardholder information (receipts, reports, supporting documentation, etc.) must be secured and limited to only those individuals whose job requires such access.

- Strict control must be maintained over any media containing cardholder data.

- Physically secure paper media containing sensitive cardholder data at all times (e.g. locked down) and safeguard it if being transported. A secure location would minimally be defined as one that is not accessible to the public, particularly if authorized personnel are not always available to monitor security.

- Destroy media containing cardholder data when no longer needed in accordance with PCI DSS guidelines.

- Secure locations must have physical access controls (key cards, door locks, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security.

- Develop procedures to help all personnel easily distinguish between employees and visitors.

Personnel Access Control

- Passwords must be added for refunds/voids (used by someone other than who is processing charges)

- Restrict access to cardholder data by business need-to-know basis.

- Limit access to system components and cardholder data to only those individuals whose job requires such access.

- Restrict access rights to privileged user IDs to the least privileges necessary to perform job responsibilities.

- Assign privileges based on individual personnel's job classification and function.

- Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to deny all unless specifically allowed.

Storage of Cardholder Data

- Keep cardholder information storage to a minimum. Storage of sensitive cardholder data on any local device or system is prohibited.

- Do not store the Card Verification Value (three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data).

- Ensure secure storage and distribution of university keys.

- Periodically change keys and destroy old keys.

- An inventory **must** be maintained of all systems, electronic, and paper media containing sensitive cardholder data.

Transmission and Distribution of Cardholder Data

- All transmission and distribution of sensitive cardholder data must use a secure method to avoid unauthorized access.

- Never send or accept cardholder or other sensitive information via unencrypted e-mail, Instant Messaging or any other insecure method (e.g. File Transfer Protocol (FTP), Hypertext Transport Protocol etc.).

- Mask the credit card's Primary Account Number (PAN) when displayed.

Protecting Cardholder Data

- When sensitive authentication data is received and deleted, there must be a process in place to securely delete the data and to assure the data is unrecoverable.

- All systems must adhere to the PCI DSS requirements regarding non-storage of sensitive authentication data after authorization.

- Under **no** circumstance, should the full contents of any track from the magnetic stripe be stored.

  In the normal course of business, the following data elements from the magnetic stripe may need to be retained. To minimize risk, store only these data elements as needed for business.

    - *The cardholder's name*
    - *Primary account number (PAN)*
    - *Expiration Date*

- Under **no** circumstance should the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) be stored.

- Under **no** circumstance should the personal identification number (PIN) or the encrypted PIN block be stored.

Maintain an Information Security Policy
All merchants should maintain a policy that addresses information security for all personnel. "Personnel" refers to full time and part time employees, temporary employees, contractors and consultants have access to the cardholder data environment.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

The security policy should be reviewed at least once a year and updated as needed to reflect any changes to business objectives or the risk environment.

Disposal and Re-Use of Hardware, Electronic and Paper Media

- Hardcopy media must be destroyed when it is no longer needed for business or legal reasons. It is recommended that it be held in case a refund request or chargeback dispute comes through but no longer than six to twelve months from the date of the transaction.

- Destruction of hardcopy media must be cross-cut shredded, incinerated or pulped so that cardholder data cannot be reconstructed. If this is not possible, credit card numbers and personal information must be "blacked-out" before destroying.

- Containers that store cardholder data to be destroyed must be secured to prevent access to the contents. Example: a "to-be-shredded" container must have a lock preventing access to its contents.

- Shred, incinerate, pulp or "black-out" paper media containing cardholder data so that it cannot be reconstructed.

Incident Reporting

In the event of a security breach in which a person's Personal Information is reasonably believed to have been stolen by an unauthorized person, the breach must be reported immediately to a supervisor and:

- The Campus Credit Card Coordinator
  cashandmerchant@ucr.edu
  (951) 827-3991

In the event of a compromise involving credit card information, encrypted or unencrypted, it is critical to immediately report the breach to a supervisor and:

- The Campus Credit Card Coordinator
  cashandmerchant@ucr.edu
  (951) 827-3991

References:
PCI DSS - https://www.pcisecuritystandards.org/security_standards/index.php
BUS-49 - http://policy.ucop.edu/doc/3420337/BFB-BUS-49

I have thoroughly read the Terminal Control Measures and understand that I must follow PCI DSS and BUS-49 requirements in the handling of credit card data. My department accepts full responsibility should a breach occur due to employee negligence or fraud in the mishandling of cardholder information. Campus Credit Card Coordinator reserves the right to suspend or terminate service at any time if sufficient security measures are not employed by my department.

***By signing below, I understand my role and responsibilities as a merchant*.**

Signature: _____ **Date:** _____
Department Representative

Department Name/Title and Ext: _____