UCLA Policy 314 Payment Card Processing Standards

Issuing Officer:	Associate Vice Chancellor, Corporate Financial Services
Responsible Dept:	Corporate Financial Services
Effective Date:	October 19, 2011
Supersedes:	New

I. REFERENCES

1. UC Business and Finance Bulletin BUS-49, Policy for Cash and Cash Equivalents Received;
2. Payment Card Industry Data Security Standard (PCI DSS);
3. UCLA Policy 404, Protection of Electronically Stored Personal Information;
4. UCOP, IR&C Guidelines: Protecting University Data Through Agreements or Contracts with Third-Party Vendors.

II. PURPOSE

The purpose of this policy is to ensure that the appropriate minimum security standards for processing credit and debit card information at UCLA are identified and adhered to, and that prior approval is secured before credit and debit card (hereinafter payment card) transactions can be executed

This policy applies to all employees who process payment card information, including students, full time, part-time and temporary employees, the workforce of the UCLA Health System; and all third parties who process payment card information whose conduct in the performance of their work for UCLA is under the control of UCLA or the Regents of the University of California.

III. DEFINITIONS

For the purposes of this Policy, the following terms shall apply:

Attestation of Compliance (AOC) means a self-certification that a unit or department has signed attesting to the fact that it has adhered to Payment Card Industry Data Security Standard.

Cardholder Data means the primary payment card account number, the cardholder name, the expiration date and the service code as defined in the Payment Card Industry Data Security Standard.

Payment Coordinator is the Director of Student Financial Services in Corporate Financial Services.

Self-Assessment Questionnaire (SAQ) means a validation tool to assist a unit or department in self-evaluating itself to verify that it adheres to the Payment Card Industry Data Security Standard.

IV. STATEMENT

The proper collection and security of personal information gathered in the course of University business is of paramount importance. The University is obligated by policy and law to protect such information (see UCLA Policy 404 for more information).

UC Business & Finance Bulletin, BUS-49, Appendix B states in part:

> Any credit or debit card cardholder information collected, stored, or transmitted as part of a card transaction is further regulated under the Payment Card Industry (PCI) Data Security Standards (DSS). Compliance with these standards is mandatory for all University units accepting credit/debit cards for payment. Failure to comply can result in significant fines and loss of the ability to process such transactions. University units processing card transactions must understand the data security rules applicable to their processing environment. The Credit Card/Internet Payment Gateway Coordinator assists in that training as part of authorizing the unit to process cards.

No UCLA employee or third party payment processor engaged by UCLA may process or accept payments by payment card without prior approval of the campus Credit Card/Internet Payment Gateway Coordinator (hereinafter Payment Coordinator) which will be dependent upon meeting the following requirements:

- Completing the appropriate Self-Assessment Questionnaire (SAQ).
- Completing the appropriate Attestation of Compliance (AOC).
- Payment Coordinator approval of the SAQ and AOC.
- Completing annual training of all personnel with access to Cardholder Data. This includes, but is not limited to, programmers, front line cashiers, back office personnel, and anyone with access to Cardholder Data.
- For areas requiring SAQ C, C-VT or D, completing annual audits by UCLA Internal Audit and Advisory Services in order to retain PCI certification.
- If an area has a valid business need to use a third party processor which is not currently UC approved, obtaining a variance to policy from the Payment Coordinator. In addition, the third party processor must be listed as compliant on the PCI or VISA website or provide quarterly compliance updates, after approval by the Payment Coordinator.

A. Roles and Responsibilities

Unit or Department Head

Unit or Department Heads may delegate authority for administering the PCI DSS for their areas of responsibility, but are ultimately responsible for compliance with this Policy.

Unit and Department Heads must ensure that affected staff and third party vendors are thoroughly trained, that related IT support systems are tested and verified, that corrective action is taken on a timely basis to bring any processes into compliance which are found to be deficient.

Any fines or costs that are assessed related to non-compliance will be borne by the affected unit or department.

Payment Coordinator

The Payment Coordinator has sole authority for approving or denying requests for the acceptance of payment for goods or services via payment cards. She or he may rescind the acceptance of payment card transactions of a unit or department found to be non-compliant.

The Payment Coordinator is the final authority for determination of the appropriate SAQ and AOC for completion by the unit. This may be done after consultation with the Director, IT Security.

Employees and Third Party Vendors

Employees and third party vendors must comply with all requirements of the PCI standard, specifically following established campus and departmental policy, annual training, and completion of the required SAQ and AOC, as appropriate.

IT Support Staff

IT support staff must also adhere to the PCI requirements, which include compliance with established campus and departmental policy, annual training, completion of the required SAQ and AOC, as appropriate.

B. Consequences of Non-Compliance

Failure to comply with PCI DSS requirements carries severe consequences including:

- the loss of the ability to process payment card transactions;
- litigation, insurance claims, regulatory notification requirements, potential financial liabilities (regulatory and other fees and fines);
- reputational damage and loss of customers.

Any fines and/or penalties associated with non-compliance with the PCI DSS, and/or confirmed security breaches are defined by each of the payment card brands. For more specific information, the individual payment card brand may be contacted, or by consult with the Payment Coordinator.

A lapse in compliance that results in a security breach of Cardholder Data or other covered personal information must be reported to the Director, IT Security immediately. See UCLA Policy 420 for more information.

V. ATTACHMENTS

A. PCI/DSS Self-Assessment Questionnaires and Attestations of Compliance

Issuing Officer

/s/ Allison Baird-James

Associate Vice Chancellor, Corporate Financial Services

Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.

Payment Card Industry (PCI) Data Security Standard (DSS)
Self-Assessment Questionnaires and Attestations of Compliance

The Payment Card Industry Data Security Standard requirements vary depending on the method of credit and debit card processing being used. The different methods are defined in the Self-Assessment Questionnaires (SAQ) as follows:

- SAQ A: All Cardholder Data functions outsourced. No Electronic Storage, Processing, or Transmission of Cardholder Data
    - The organization does not store, process or transmit any Cardholder Data on organization systems or premises but relies entirely on a third party service provider to handle these functions.
    - The third party service provider handling storage, processing, and/or transmission of Cardholder Data is confirmed to be PCI DSS compliant.
    - The organization does not store any Cardholder Data in electronic format.
    - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.
- SAQ B: Imprint Machines or Standalone Dial-out Terminals Only, No Electronic Cardholder Data Storage.
    - The organization uses only an imprint machine to imprint customers' payment card information and does not transmit Cardholder Data over either a phone line or Internet, or,
    - An organization uses only standalone, dial-out terminal which is not connected to the Internet or any other systems within the organization environment.
    - The organization does not store Cardholder Data in electronic format.
    - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.
- SAQ C: Payment Application Connected to the Internet, No Electronic Cardholder Data Storage
    - The organization has a payment application system and an Internet or public network connection on the same device.
    - The payment application system is not connected to any other system within the organization environment.
    - The organization's store is not connected to other store locations and any network is for a single store.
    - The organization does not store Cardholder Data in electronic format.
    - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.
    - The organization's payment application software vendor uses secure techniques to provide remote support to the organization's payment application system.
- SAQ C-VT: Web-Based Virtual Terminal, No Electronic Cardholder Data Storage
    - The organization's only payment processing is via a virtual terminal access by an Internet connected web browser.
    - The organization accesses the virtual terminal via a computer that is isolated in a single location, and is not connected to other locations or systems within the organization's environment.
    - The organization's virtual terminal solution is provided and hosted by a PCI DSS validated third party service provider.
    - The organization's computer does not have software installed that causes Cardholder Data to be stored.

  - The organization's computer does not have any attached hardware devices that are used to capture or store Cardholder Data.
  - The organization does not receive or transmit Cardholder Data electronically except through the virtual terminal.
  - The organization does not store Cardholder Data in electronic format.
  - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.
- SAQ D: Electronic Storage of Cardholder and Service Providers
  - All other organizations not meeting the requirements of a SAQ A, SAQ B, SAQ C or SAQ C-VT in addition to all service providers. This includes all organizations that retain Cardholder Data.