California State University Northridge	**Information Technology Standard Operating Procedure** PCI Compliance Review Process	**Page** 1 of 6	
		SOP#: ITIS-90-09-037	**Revision#:** Version 1.0

Prepared by: Leigh Lopez **Date:** June 18, 2009	**Approved by:** Dr. Robert Barker, University Controller **Date:** June 26, 2009
Last revised by: Leigh Lopez, Information Security Lead **Date:** August 22, 2012	**Last approved by:** Deborah Wallace, AVP Financial Services **Date:** August 23, 2012

1.0 PURPOSE

Accepting payment cards as a form of payment has a number of requirements intended to safeguard payment card information. Payment cards include credit cards, bank debit cards, check authorization cards and pre-paid cards used for cash-less transactions.

This process is intended to identify the process that CSUN state and auxiliary departments that accept or want to accept payments by payment cards must follow. These requirements also apply to departments that accept payment card information for activities such as fund raising to be passed on to another department for processing.

2.0 SCOPE

All departments and systems within the CSUN network that store, process or transmit Primary Account Numbers (credit card numbers), and all systems that are within the same logical network as these, must be in compliance with the PCI Data Security Standard.

3.0 RESPONSIBILITIES

Entity	Title	Role
Internal Audit	Internal Auditor	Audit CSUN's PCI-compliance review.
Information Technology	Information Security Officer	IT Security Administrator
	Information Security Lead or Analyst	IT Security Technical Advisor
Associated Students Inc.	Director of Accounting	Business Owner
	Technology Support Coordinator	Technical Contact
Foundation	Advancement Resources	Business Owner
	Senior Systems Analyst	Technical Contact
State Entities	AVP, Financial Services	Business Owner
	Senior Systems Analyst	Technical Contact
University Corporation	Facilities & Project Manager	Business Owner
	Senior Systems Analyst	Technical Contact
University Student Union	Associate Director, Finance	Business Owner
	Technology Support Services Manager	Technical Contact

AVP of Financial Services (or designee) – The role of the AVP of Financial Services is to oversee CSUN's PCI- Compliance Process; to ensure the appropriate self-assessment questionnaires are submitted to the acquiring banks in a timely manner; and in conjunction with the ISO and Business Owners, identify remediation dates for areas of noncompliance.

Information Security Officer (or designee) – The role of the Information Security Officer (ISO**)** is to ensure that both the requisite PCI Annual Penetration Test and Quarterly Scans are conducted consistent with the requirements set forth in the PCI DSS 1.2; to provide direction for the technical remediation, and to provide oversight for the vendor scanning/testing engagements. In conjunction with the AVP for Financial Services, identify remediation action plan dates for areas of technical non-compliance on the SAQs.

IT Network Engineer – Maintain the network zone/segments to provide PCI-mandated levels of protection for campus PCI devices. Place new PCI devices into the appropriate network/zone segment.

Business Owner – The role of the 'Business Contact' is to:

1. Complete and sign the self-assessment questionnaire ("SAQ"):

   Part 2 – *Merchant Organization Information*
   - ***2A*** *- Type of Merchant Business*
   - ***2B*** *– Relationships*
   - ***2C –*** *Transaction Processing*

- ***2D*** *– Eligibility to Complete SAQ Type*

Part 3 – PCI DSS Validation

- ***3A*** *– Confirmation of Compliance Status*
- ***3B*** *– Merchant Acknowledgement*

2. Ensure the timely remediation of vulnerabilities for department PCI devices. Detailed vulnerability reports will be provided quarterly by the Information Security office following each campus- and ASV-PCI vulnerability-scan.

   - In response to campus vulnerability scans: remediate findings prior to the ASV (official/vendor) scans;
   - Authorized Scanning Vendor (ASV) scans – remediate findings prior to subsequent ASV scans.

Information Security Lead or Analyst – The role of the Information Security Lead or Analyst is to conduct the campus-originated (preventative) quarterly internal and external vulnerability scans of campus PCI devices; coordinate with business and technical contacts to 1) remediate vulnerabilities, 2) assist with completion of the PCI-DSS SAQ sections that pertain to campus IT services/policies; 3) coordinate with ASV technical staff to conduct ASV-conducted (official) quarterly and annual vulnerability and penetration tests, 4) Identify areas of PCI non-compliance and bring to the attention of the ISO and AVP for Financial Services. Areas of non-compliance will require a remediation action plan date on the respective SAQs.

Technical Contact – Remediate vulnerabilities pertaining to PCI devices. Assist business contacts and Information Security with completing the technical components on the SAQs. Inform Information Technology when new PCI devices are introduced to the campus network so that they can be added to the appropriate network zone/segment.

4.0 PROCESS

1. In accordance with the time table below, in preparation for the PCI-required quarterly external vulnerability scan (to be run by an ASV) and annual penetration test, the Information Security Analyst will conduct internal and external vulnerability scans against CSUN's Credit Card Processing/PCI network to identify known and potential vulnerabilities. Vulnerability reports will be distributed to the respective PCI business and technical contacts for remediation.

Vulnerability and Penetration Scan Time Table		
Quarter	**Timeframe**	**Scan**
	1st week of the each month	CSUN Vulnerability Scan Monthly (preventative)
	Monthly between each scan	Remediate
	Last week of each quarter	ASV PCI-Required External Vulnerability Scan and Submittal to acquiring bank(s)

2. September of each calendar year, the AVP of Financial Services (or designee) holds a kickoff meeting with the PCI workgroup, which consist of the ISO (or designee), the IT/Information Security Lead or Analyst, and the business contact for each campus PCI department. The purpose of the meeting is to review the process for conducting the annual PCI compliance review.

3. Business owners review prior year Self-Assessment Questionnaires (SAQs). Business owners review the prior year Self-Assessment Questionnaires (SAQs) and complete the current year SAQ.
    a. Contact acquiring banks to determine the appropriate SAQ to complete;
    b. Complete the SAQs. Coordinate as needed with department IT personnel and central-IT assist with the technical related sections.
    c. Identify areas of noncompliance and coordinate with the responsible areas to identify project remediation dates.
    d. Sign and submit the SAQs to the acquiring banks.

CSUN Payment Card Industry (PCI)/ Credit Card Contacts

Owner	Department	Title
Associated Students Inc.		Director of Accounting
		Manager of Support Services
Foundation	Foundation	Asst. VP for Resource Mgmt., Advancement Resources
	University Advancement	Assoc VP for Development, Advancement Resources
	KCSN	General Manager, KCSN
	KCSN	Membership/Underwriting
State Entities	State	AVP for Financial Services
	State	Manager, Cash Services
	Financial & Tax Services	Assistant Director
	Student Accounting	Third Party Sponsor Coordinator
	Public Safety Parking	Captain
	Center on Disabilities	Accounting Manager
	National Center on Deafness	Admin of Finance & Technology
	Quickcopies	Director
	Quickcopies	Duplicating Machine Supervisor I
	Res Life & Conf Admin	Financial Analyst
	ExL, Financial & Fiscal Management	Asst. Director
	Student Health Center	Assistant Director, Ancillary Svcs
University Corporation		Facilities & Project Manager
University Student Union		Associate Director, Finance

5.0 DEFINITIONS:

Vulnerability Scan – Nonintrusive test that probes external-facing systems and reports on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network and credit card data.

Penetration Test – Method of evaluating the security of a computer system or network by simulating a controlled attack against a known vulnerability. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

PCI DSS – The Payment Card Industry Data Security Standard is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council. The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

6.0 REFERENCES:

The following documents were created to assist departments/units and service providers in understanding the PCI Data Security Standard and the PCI DSS SAQ.

PCI Data Security Standard Documentation - http://goo.gl/Ks8N9