

**AUXILIARY ORGANIZATIONS**

**CALIFORNIA POLYTECHNIC STATE UNIVERSITY,  
SAN LUIS OBISPO**

**Audit Report 08-51  
February 4, 2009**

---

**Members, Committee on Audit**

Melinda Guzman, Chair  
Raymond W. Holdsworth, Vice Chair  
Herbert L. Carter   Kenneth Fong  
Margaret Fortune   George G. Gowgani  
William Hauck   Henry Mendoza

---

**Staff**

University Auditor: Larry Mandel  
Senior Director: Janice Mirza  
Audit Manager: Gary Miller  
Senior Auditors: Kwabena Boakye and Ken Tsui  
Internal Auditors: Jamarr Johnson, Julia Mathis, and Kathy Schaeffer

---

**BOARD OF TRUSTEES  
THE CALIFORNIA STATE UNIVERSITY**

---

## CONTENTS

Executive Summary .....	1
Introduction.....	5
Background.....	5
Purpose .....	6
Scope and Methodology .....	7

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

### **CAMPUS**

Fees, Revenues, and Receivables.....	10
--------------------------------------	----

### **CAL POLY CORPORATION**

Operational Compliance .....	12
Segregation of Duties.....	13
Fees, Revenues, and Receivables.....	14
Purchasing and Accounts Payable .....	15
Property and Equipment .....	16
Auxiliary Programs.....	17
Information Technology .....	18
Password Security.....	18
Unique User IDs .....	20
User Access Reviews.....	20
Information Security Training .....	21
Protected Data Assessment.....	22
System Backups.....	24
Remote Server Access .....	24
Web Application Security.....	25

### **CAL POLY HOUSING CORPORATION**

Fiscal Compliance.....	27
Segregation of Duties.....	28

**ASSOCIATED STUDENTS, INCORPORATED OF**  
**CALIFORNIA POLYTECHNIC STATE UNIVERSITY AT SAN LUIS OBISPO**

Facilities Agreements..... 29

Property and Equipment ..... 30

Information Technology ..... 31

    Password Security..... 31

    Computer Room Security ..... 32

    User Access Reviews..... 32

    Protected Data Assessment..... 33

    Web Application Security..... 34

## **APPENDICES**

APPENDIX A:	Personnel Contacted
APPENDIX B:	Statement of Internal Controls
APPENDIX C:	Campus Response
APPENDIX D:	Chancellor's Acceptance

---

## **ABBREVIATIONS**

AD	Active Directory
ASI	Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo
CFO	Chief Financial Officer
Corporation	Cal Poly Corporation
CSU	California State University
EMC	Enterprise Management Console
EO	Executive Order
Foundation	California Polytechnic State University Foundation
Housing	Cal Poly Housing Corporation
IFAS	Integrated Financial and Administrative Solution
IMS	Investment Management System
IT	Information Technology
MBS	Missouri Book System
MCS	Micros Cashiering System
RFIN	Resolution of the Committee on Finance
Telnet	Telecommunication Network
VPN	Virtual Private Network

---

## EXECUTIVE SUMMARY

In July 1981, the Board of Trustee policy concerning auxiliary organizations was adopted in the Resolution of the Committee on Finance (RFIN) 7-81-4. Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, required that the Office of the University Auditor conduct internal compliance/internal control reviews of auxiliary organizations, and the Board of Trustees instructed that such reviews be conducted on a triennial basis pursuant to procedures established by the chancellor.

California Polytechnic State University, San Luis Obispo management is responsible for establishing and maintaining an adequate system of internal compliance/internal control and assuring that each of its auxiliary organizations similarly establishes such a system. This responsibility, in accordance with California Code of Regulations, Title 5, Section 42402 et seq. and Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations et seq.*, includes requiring the documentation of internal control, communicating requirements to employees, and assuring that its system of internal compliance/internal control is functioning as prescribed. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control procedures.

The objectives of a system of internal compliance/internal control are to provide management with reasonable, but not absolute, assurance that:

- ▶ Auxiliary operations are conducted in accordance with policies and procedures established in the State Administrative Manual, Education Code, Title 5, and Trustee policy.
- ▶ Assets are adequately safeguarded against loss from unauthorized use or disposition.
- ▶ Transactions are executed in accordance with management's authorization and recorded properly to permit the timely preparation of reliable financial statements.

We visited the California Polytechnic State University, San Luis Obispo campus and its auxiliary organizations from September 29, 2008, through October 30, 2008, and made a study and evaluation of the system of internal compliance/internal control in effect as of October 30, 2008. This report represents our triennial review.

Our study and evaluation at the *California Polytechnic State University Foundation* did not reveal any major findings or significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. In our opinion, the accounting and administrative control in effect as of October 30, 2008, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at the *Cal Poly Corporation* did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative

control in effect as of October 30, 2008, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at the *Cal Poly Housing Corporation* did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative control in effect as of October 30, 2008, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at the *Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo* did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative control in effect as of October 30, 2008, taken as a whole, was sufficient to meet the objectives stated above.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

The following summary provides management with an overview of conditions requiring their attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

## **CAMPUS**

### **FEES, REVENUES, AND RECEIVABLES [10]**

Campus matching gift procedures did not require that a documented dual review be performed prior to the deposit of matching gift funds.

## **CAL POLY CORPORATION**

### **OPERATIONAL COMPLIANCE [12]**

The Cal Poly Corporation (Corporation) had not developed policies and procedures to address the management and/or control of inventory waste, spoilage, and shrinkage related to dining and bookstore operations.

### **SEGREGATION OF DUTIES [13]**

Duties, responsibilities, and system access for certain purchasing and administrative functions were not adequately segregated at the Corporation.

### **FEES, REVENUES, AND RECEIVABLES [14]**

Reconciliations between the Corporation general ledger accounting system and certain bookstore systems were not signed and dated by the preparer and reviewer to evidence timely completion and independent review.

### **PURCHASING AND ACCOUNTS PAYABLE [15]**

Certain Corporation cash disbursements were not supported by sufficient and appropriate documentation or were not timely paid.

### **PROPERTY AND EQUIPMENT [16]**

Administration of Corporation property and equipment needed improvement. This is a repeat finding from the prior auxiliary organizations audit that was reported for the Foundation, which was previously responsible for commercial operations.

### **AUXILIARY PROGRAMS [17]**

The Corporation had not performed a review of its custodial trust accounts to determine the source of deposits and whether state funds were being inappropriately maintained within these accounts.

### **INFORMATION TECHNOLOGY [18]**

Password security parameters were not always adequate for Corporation systems, and cashiers were not provided with unique user account IDs for login at registers within the Micros Cashiering System to localize transaction accountability to specific employees. Further, the Corporation did not perform a periodic documented management review of user access privileges within all systems and applications containing protected data or a periodic assessment and inventory of protected information residing on its systems, and Corporation employees with access to critical systems or protected data were not required to complete information security awareness training. In addition, daily, weekly and monthly backups for Corporation systems with protected data were not encrypted when stored locally or when in transit for off-site disaster recovery purposes, remote access to Corporation servers was not always secure, and the evaluation/testing of the quality and security of web applications prior to moving them into production was not formally documented.

## **CAL POLY HOUSING CORPORATION**

### **FISCAL COMPLIANCE [27]**

The Cal Poly Housing Corporation (Housing) had not developed a reserve policy.

### **SEGREGATION OF DUTIES [28]**

Duties and responsibilities over certain purchasing and payables/disbursement functions were not adequately segregated at Housing.

## **ASSOCIATED STUDENTS, INCORPORATED OF CALIFORNIA POLYTECHNIC STATE UNIVERSITY AT SAN LUIS OBISPO**

### **FACILITIES AGREEMENTS [29]**

Certain lease agreements between the Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo (ASI) and the campus expired.

### **PROPERTY AND EQUIPMENT [30]**

The annual ASI property reconciliation for fiscal year 2007/08 was not signed and dated by the preparer and reviewer to evidence timely completion and independent review.

### **INFORMATION TECHNOLOGY [31]**

Password security parameters were not always adequate for ASI systems, and there was no fire extinguisher in the ASI server room. In addition, the ASI did not perform a periodic documented management review of user access privileges within all systems and applications containing protected data or a periodic assessment and inventory of protected information residing on its systems. Also, the ASI did not formally document the evaluation/testing of the quality and security of web applications prior to moving them into production.

---

## INTRODUCTION

### **BACKGROUND**

Education Code §89900 states, in part, that the operation of auxiliary organizations shall be conducted in conformity with regulations established by the Trustees.

Education Code §89904 states, in part, that the Trustees of the California State University (CSU) and the governing boards of the various auxiliary organizations shall:

- ▶ Institute a standard systemwide accounting and reporting system for businesslike management of the operation of such auxiliary organizations.
- ▶ Implement financial standards that will assure the fiscal viability of such various auxiliary organizations. Such standards shall include proper provision for professional management, adequate working capital, adequate reserve funds for current operations and capital replacements, and adequate provisions for new business requirements.
- ▶ Institute procedures to assure that transactions of the auxiliary organizations are within the educational mission of the state colleges.
- ▶ Develop policies for the appropriation of funds derived from indirect cost payments.

The Board of Trustee policy concerning auxiliary organizations was originally adopted in July 1981 in the Resolution of the Committee on Finance (RFIN) 7-81-4. Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, represents policy of the Trustees addressing CSU auxiliary organization activity and governing the internal management of the system. CSU auxiliary organizations are required to comply with Board of Trustee policy (California Code of Regulations, Title 5, Section 42402 and Education Code, Section 89900).

This executive order requires that the Office of the University Auditor will perform an internal compliance/internal control review of auxiliary organizations. The review will be used to determine compliance with law, including statutes in the Education Code and rules and regulations of Title 5, and compliance with policy of the Board of Trustees and of the campus, including appropriate separation of duties, safeguarding of assets, and reliability and integrity of information. According to Board of Trustee instruction, each auxiliary organization shall be examined on a triennial basis pursuant to procedures established by the chancellor.

The California Polytechnic State University Foundation (Foundation) acts as the philanthropic auxiliary for the campus. The sole function of the Foundation is to collect, invest, and administer all gifts, bequests, endowments, trusts, and similar funds received by the campus. Fund-raising activities of the Foundation are carried out by board members and other volunteers under the general direction of the board development committee and with support from university advancement staff. The vice president of university advancement provides campus oversight to the Foundation and the Cal Poly Corporation performs all accounting functions. Since our last review in December 2005, commercial operations such

as campus dining and the bookstore were transferred from the Foundation to the Cal Poly Corporation in February 2006.

The Cal Poly Corporation (Corporation) acts as the primary entity responsible for commercial operations, which include the El Corral Bookstore, campus dining, university graphics systems, sponsored programs, and a host of other programs. The Corporation has complete administrative responsibility for these operations and programs. The Corporation, in cooperation with the appropriate campus administrative offices, provides fiscal services to instructionally related programs, conferences, workshops, and institutes to supplement the instructional programs, and agency activities as requested by the university. The Corporation also provides fiscal administration and support services for grants and contracts for research, instruction, and public service, private gifts to the university, and other support sources. Since our last review in December 2005, all commercial operations, sponsored programs and other agency activities, with the exception of gift administration, were transferred from the Foundation to the Corporation in February 2006. In addition to the changes in operations, the Corporation experienced significant turnover within upper management.

The Cal Poly Housing Corporation (Housing) is organized as a non-profit public benefit corporation for the purposes of the development, provision, and maintenance of affordable housing and other related facilities and activities for the use and convenience of faculty, staff, and students of the university, in order to foster an academic community and environment on or near the campus, and to attract and retain the highest quality faculty, staff, and students at the university. Incorporated in June 2001, Housing completed construction in September 2007 of 69 attached homes for use as faculty and staff housing.

The Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo (ASI) is the campus auxiliary charged with operating the student body government, University Union facilities, the Children's Center, and Poly Escapes. Each year the student body holds elections to select new officers. The president of the ASI is the chief executive of the auxiliary, although the ASI does employ an executive director to manage day-to-day operations and provide consistency between student administrations. The ASI is also responsible for the fiscal administration of student organizations.

## **PURPOSE**

The principal audit objectives were to determine compliance with the Education Code, Title 5, and directives of the Board of Trustees and the Office of the Chancellor and to assess the adequacy of controls and systems. Specifically, we sought assurances that:

- ▶ Legal and regulatory requirements are complied with.
- ▶ Accounting data is provided in an accurate, timely, complete, or otherwise reliable manner.
- ▶ Assets are adequately safeguarded from loss, damage, or misappropriation.
- ▶ Duties are appropriately segregated consistent with appropriate control objectives.
- ▶ Transactions, accounting entries, or systems output is reviewed and approved.
- ▶ Management does not intentionally override internal controls to the detriment of control objectives.
- ▶ Accounting and fiscal tasks, such as reconciliations, are prepared properly and completed timely.

- ▶ Deficiencies in internal controls previously identified were corrected satisfactorily and timely.
- ▶ Management seeks to prevent or detect erroneous recordkeeping, inappropriate accounting, fraudulent financial reporting, financial loss, and exposure.

## **SCOPE AND METHODOLOGY**

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that accounting and administrative controls are in place and operative. The management review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. For those audit tests that required annualized data, fiscal years 2006/07 and 2007/08 were the primary periods reviewed. In certain instances, we were concerned with representations of the most current data; in such cases, the test period was October 31, 2007, to October 30, 2008. Our primary focus was on internal compliance/internal control.

Specifically, we reviewed and tested:

- ▶ Formation of the auxiliary.
- ▶ Functions the auxiliary performs on the campus.
- ▶ Creation and operation of the auxiliary's board.
- ▶ Establishment of policies and procedures based upon sound business practices.
- ▶ Maintenance of "arms-length" in business transactions between the auxiliary and the campus.
- ▶ Campus oversight of auxiliary operations.

Additionally, for the period reviewed, we examined other aspects of compliance of the campus and each auxiliary with the Education Code and Title 5 as they relate to the operation of CSU auxiliary organizations. Individual codes and regulations added to the scope of our review were identified through an assessment of risk. Similarly, internal controls were included within our scope based upon risk. Therefore, the scope of our review varied from auxiliary to auxiliary.

A preliminary survey of CSU auxiliaries at each campus was used to identify risks. Risk was defined as the probability that an event or action would adversely affect the auxiliary and/or the campus. Our assessment of risk was based upon a systematic process, using professional judgments on probable adverse conditions and/or events that became the basis for development of our final scope. We sought to assign higher review priorities to activities with higher risks. As a result, not all risks identified were included within the scope of our review.

Based upon this assessment of risks, we specifically included within the scope of our review the following:

California Polytechnic State University Foundation

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Endowment Administration

Cal Poly Corporation

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Endowment Administration
- ▶ Auxiliary Programs
- ▶ Information Technology

Cal Poly Housing Corporation

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Cash Receipts and Handling

Cal Poly Housing Corporation (cont.)

- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs

Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs
- ▶ Information Technology

Campus

- ▶ Campus Oversight and Control

We have not performed any auditing procedures beyond October 30, 2008. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.

---

# OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

## CAMPUS

### FEES, REVENUES, AND RECEIVABLES

The administration of matching gifts required improvement.

We found that the campus matching gift procedures did not require that a documented dual review be performed prior to the deposit of matching funds to a specifically directed recipient to ensure that funds are appropriately deposited with an eligible recipient in accordance with corporate donor requirements.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the California State University (CSU) system. Section 8.9.3, *Donations, Program Service Fees, Other Income*, states that the auxiliary should establish a written recordkeeping system that enables gifts to be properly received, recorded, and acknowledged in accordance with donor restrictions and other requirements.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates matching gifts undergo a dual review process to ensure that funds are appropriately deposited to an eligible recipient in accordance with corporate donor requirements.

The Foundation chief financial officer (CFO) stated that he was unaware of any prior written guidance from the CSU or recognized best practice regarding a dual review to ensure that funds are appropriately deposited with an eligible recipient in accordance with corporate donor requirements but agreed to work with the campus to implement the recommended dual review.

Insufficient administration of matching gifts increases the likelihood of misdirected funds and campus exposure to liabilities from non-compliance with corporate donor policies.

#### **Recommendation 1**

We recommend that the campus improve the matching gifts policy to ensure that a secondary eligibility review is documented prior to the deposit of matching funds to a specifically directed recipient.

**Campus Response**

We concur. Senior university advancement services staff are now conducting a secondary review of all matching gifts prior to the deposit of matching funds. This item has been completed.

## **CAL POLY CORPORATION**

### **OPERATIONAL COMPLIANCE**

The Cal Poly Corporation (Corporation) had not developed policies and procedures to address the management and/or control of inventory waste, spoilage, and shrinkage related to dining and bookstore operations.

Specifically, policies and procedures should address:

- ▶ Development of acceptable levels of inventory waste, spoilage, and shrinkage and guidelines for action required when these levels are exceeded.
- ▶ Recording the type and cost of inventory waste, spoilage, and shrinkage generated by each operation.
- ▶ Periodic management review of inventory waste, spoilage, and shrinkage data.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the development of policies and procedures to address inventory waste, spoilage, and shrinkage.

The Corporation associate director of campus dining stated that inventory waste and spoilage procedures were followed and budgets were prepared based on prior year numbers, although written procedures had not been prepared. The Corporation El Corral Bookstore associate director of operations stated that although there was no policy, they budgeted for inventory shrinkage at 0.5 percent of sales.

The absence of written policies and procedures to address the management and/or control of inventory waste, spoilage, and shrinkage related to dining and bookstore operations increases the risk of errors or misappropriation.

#### **Recommendation 2**

We recommend that the Corporation develop policies and procedures to address the management and/or control of waste, spoilage, and shrinkage related to dining and bookstore operations.

### **Campus Response**

We concur. We will write new procedures to address how the amount for shrinkage is determined, reviewed, and adjusted as part of dining and bookstore annual inventory processes.

Completion: July 31, 2009

### **SEGREGATION OF DUTIES**

Duties, responsibilities, and system access over certain purchasing and administrative functions were not adequately segregated at the Corporation.

We found that the campus dining purchasing manager:

- ▶ Had access to the Eatec dining services system to enter and approve purchase orders and enter receiving data.
- ▶ Approved invoices for payment.
- ▶ Prepared the physical inventory variance (shrinkage) analysis.

Executive Order (EO) 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.5, *Procurement*, states, in part, that the auxiliary should establish a written internal controls system that provides purchase orders and service contracts are prepared separately from both receiving and shipping, and payables and disbursements.

The Corporation campus dining director stated that although the purchasing manager had the capability of performing the cited functions as the administrator of the Eatec system, she was not responsible for performing all of those functions in order to keep activities segregated. He further stated that the purchasing office staff entered purchase orders and receiving data, but duties were administratively divided with the food buyer entering purchase orders and the campus dining secretary and her assistant entering the receiving data. He added that the purchasing manager did prepare the physical inventory variance analysis, but did not perform the inventory.

Inadequate segregation of duties increases the risk that errors and irregularities will not be detected in a timely manner.

### **Recommendation 3**

We recommend that the Corporation restrict the campus dining purchasing manager's access to the Eatec dining services system or institute mitigating procedures approved by the campus CFO.

#### **Campus Response**

We concur. Corporation management will restrict the campus dining purchasing manager's access to enter purchase orders and receiving data into the Eatec system and will enhance existing procedures to limit the risk of errors and irregularities.

Completion: July 31, 2009

## **FEES, REVENUES, AND RECEIVABLES**

Reconciliations between the Corporation general ledger accounting system and certain bookstore systems were not signed and dated by the preparer and reviewer to evidence timely completion and independent review.

Specifically, monthly reconciliations between the general ledger and the bookstore cashiering system and the Missouri Book System (MBS) were not signed and dated by the preparer and reviewer to evidence timely completion and independent review.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient documentation of timely preparation and independent review of account reconciliations.

The Corporation CFO stated that the reconciliations were completed by the appropriate Corporation staff according to current practices, but current procedures did not require signatures to evidence completion of the reconciliation process.

Failure to sufficiently document account reconciliations increases the risk that errors and irregularities will not be timely detected and accountability will not be maintained.

### **Recommendation 4**

We recommend that the Corporation ensure that reconciliations between the general ledger accounting system and the bookstore cashiering system and the MBS be signed and dated by the preparer and reviewer.

### **Campus Response**

We concur. Effective February 1, 2009, we implemented a procedure that requires staff preparing and reviewing reconciliations to sign and date these documents.

## **PURCHASING AND ACCOUNTS PAYABLE**

Certain Corporation cash disbursements were not supported by sufficient and appropriate documentation or were not timely paid.

Our review of 60 cash disbursements ranging from April 11, 2006, through June 27, 2008, disclosed the following:

- ▶ In three instances, payments were issued without sufficient supporting documentation.
- ▶ In four instances, invoices were not paid timely according to vendor terms.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.1, *Cash*, states that the auxiliary should disburse cash in a consistent manner utilizing systems that ensure integrity of existing controls, with annual management review.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that all cash disbursements be fully supported and timely paid.

The Corporation accounting project manager stated that the three payments issued without sufficient supporting documentation were due to oversight and the four invoices were not paid according to vendor terms because the departments had not forwarded the invoices to accounts payable for processing in a timely manner. She added that the Corporation had not incurred any late fees as a result of the late payments.

Lack of sufficient and appropriate supporting documentation and untimely payments increase the risk of errors, irregularities, and misappropriation of funds.

### **Recommendation 5**

We recommend that the Corporation reiterate to staff existing cash disbursement policies and procedures regarding sufficient and appropriate supporting documentation, and timeliness of payment.

### **Campus Response**

We concur. By February 28, 2009, we will complete a review of existing policy and procedures with accounts payable staff to ensure cash disbursement documentation is complete and vendor payments are made timely.

## **PROPERTY AND EQUIPMENT**

Administration of Corporation property and equipment needed improvement.

This is a repeat finding from the prior auxiliary organizations audit that was reported for the Foundation, which was previously responsible for commercial operations. Our review of ten assets selected from the July 31, 2008, inventory report disclosed that:

- ▶ Two items were not tagged.
- ▶ One item could not be located.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should establish a written system that ensures proper labeling of equipment.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration over property and equipment.

The Corporation El Corral Bookstore associate director of operations stated that one asset was not tagged because it was no longer in use. The Corporation accounting project manager stated that the other asset was not tagged due to oversight. The Corporation accounting project manager stated that the unlocated asset might have been disposed of and not removed from inventory records.

Insufficient administration of property and equipment increases the risk that property may be lost or stolen, and misrepresented in the financial statements.

### **Recommendation 6**

We recommend that the Corporation:

- a. Ensure that all assets are tagged.
- b. Maintain accurate records of the location and disposal of all assets.

### **Campus Response**

We concur. Corporation receiving procedures will be revised to ensure all equipment is tagged and inventoried by location.

Completion: October 31, 2009

## **AUXILIARY PROGRAMS**

The Corporation had not performed a review of its custodial trust accounts to determine the source of deposits and whether state funds were being inappropriately maintained within these accounts.

We noted that, as of fiscal year end June 30, 2008, the Corporation administered and maintained numerous custodial trust accounts for campus programs, departments, colleges, and other groups. However, the Corporation had not performed an adequate review to determine whether the monies held were state funds.

EO 919, *Policy Governing Non-General Fund Receipts*, dated October 15, 2004, states that each CSU campus shall administer their non-General Fund receipts to ensure that the funds are held in proper accounts. EO 919 also states that, as a matter of CSU policy, auxiliaries may not accept state funds with the intent of administering them as an agent of the university. Payment for services is the only instance where state funds may be accepted into an auxiliary organization's account. Further, the entity that is responsible for any losses that might arise from the event or activity that generated the receipts shall be the entity wherein receipts are held.

Although EO 1000, *Delegation of Fiscal Authority and Responsibility*, dated July 1, 2007, indicates that it supersedes EO 919, the areas noted above are acknowledged by systemwide administrators to still be in effect and will be addressed by the forthcoming Integrated CSU Administrative Manual.

The Corporation CFO stated his belief that the Corporation had the authority to administer these programs and, therefore, had the authority to hold these accounts and record the funds as Corporation assets.

The campus' required oversight of state funds is limited when funds are deposited outside the custody of the CFO.

### **Recommendation 7**

With reference to the description of EO 919 cited above, we recommend that the Corporation and the campus:

- a. Work together to ensure compliance with EO 919, determine if any assets reflected in the Corporation financial statements contain state funds, and move any identified state funds to campus accounts.

- b. Certify that none of the following specific and similar monies reside in Corporation accounts:
- Gifts to the university, its units and programs.
  - Contracts and grants awarded to the university.
  - Fees for continuing education courses provided by the university.
  - Fees for university events, workshops, conferences, institutes, special projects, and programs.
  - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
  - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
  - Student fees and other general fees pursuant to the CSU student fee policy.
  - Monies held by the Corporation via contract with the campus.
- c. Provide supporting documentation to evidence the content and review of custodial trust accounts and the reason for the determination made.

### **Campus Response**

We concur that state funds should not be held by auxiliary organizations. The Corporation and the university will conduct a review to determine if any state funds reside in Corporation accounts and will transfer any state funds to the university.

Completion: December 31, 2009

## **INFORMATION TECHNOLOGY**

### **PASSWORD SECURITY**

Password security parameters were not always adequate for Corporation systems.

The following UNIX password security parameters, which enabled access to the Integrated Financial and Administrative Solution (IFAS) system and the Investment Management System (IMS), were set outside of leading security standards:

- ▶ Minimum time between password changes = 0 weeks.
- ▶ Password History Depth = two passwords.

The following manager account access security parameters to the Enterprise Management Console (EMC) of the Micros Cashiering System (MCS), which allowed managers to program changes to certain functions, were set outside of leading security standards:

- ▶ Maximum Password Length = four characters.
- ▶ Password complexity = only letters.
- ▶ Passwords never expire.
- ▶ No failed login limits (before disabling access).
- ▶ No idle time limits (before automatic log-off).

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates strong password and login parameters, and time-out settings.

The Corporation information technology (IT) manager stated that for IFAS, the Corporation chose the “zero weeks” option to allow the new users to change the password upon their initial logon as opposed to setting the parameter to “one week” (the other option), which would have required them to wait a week before they could change the default password. She further stated that the Corporation chose a lower password history depth of two in conjunction with other stronger password parameters, but had not considered the recycling of passwords permitted with this low password history depth. The Corporation IT manager also stated that several of the EMC/MCS password and login security settings were not enabled due to oversight, but added that the MCS had limitations in meeting all of the campus password requirements, such that there was no provision for special characters, upper or lower case, or a certain number of each in the password.

Insufficient password and login parameters and time-out settings may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems; all of which increase the risk of unauthorized access to auxiliary systems and confidential data.

### **Recommendation 8**

We recommend that the Corporation reassess its security requirements and set effective password security controls and time-out settings for its computer systems.

### **Campus Response**

We concur. As of October 20, 2008, we implemented enhanced password security controls by modifying the UNIX account "Password History Depth" to the maximum allowed value of 10. At the advice of the audit manager, we left the "Minimum time between password changes" as "zero weeks," as it offers better security over "one week" (the other option). This item was completed during audit field work.

## **UNIQUE USER IDS**

The Corporation did not provide cashiers with unique user account IDs for login at registers within the MCS to localize transaction accountability to specific employees.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the use of unique user accounts for all systems access.

The Corporation campus dining director stated that unique user accounts IDs were not considered a necessity since supervisors tracked who was assigned to each register and tracked any incidents of shortages and repetitive cashier errors.

Failure to properly localize user accountability for transactions and access to systems increases the risk of uncertainty for transactional errors and increases the risk of inappropriate access.

### **Recommendation 9**

We recommend that the Corporation assign unique user account IDs to all users accessing and recording transactions in the MCS.

### **Campus Response**

We concur. As of November 1, 2008, we assigned unique user IDs, and we provided training and a procedural manual to all cashiers accessing and recording transactions in the Micros Cashiering System installed at the Corporation dining venues. This item has been completed.

## **USER ACCESS REVIEWS**

The Corporation did not perform a periodic documented management review of user access privileges within all systems and applications containing protected data.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the

objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates a periodic documented review of user access privileges within all systems and applications containing protected data.

The Corporation IT manager stated that while the Corporation had developed a number of written procedures, reports, structured query language scripts, and triggers for this purpose, the Corporation had not considered a formalized process to ensure consistent and documented reviews of user access within all systems containing protected data.

Failure to periodically perform a documented review of user access to systems containing protected data increases the risk of inappropriate access.

### **Recommendation 10**

We recommend that the Corporation conduct periodic documented management reviews of user access to systems containing protected data, at least annually.

### **Campus Response**

We concur. We will formalize the procedure for reviewing user access privileges within all systems and applications containing protected data. We will document the annual management review of such information in accordance with the CSU and campus policy.

Completion: July 31, 2009

## **INFORMATION SECURITY TRAINING**

Corporation employees with access to critical systems or protected data were not required to complete information security awareness training.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic information security training for all employees with access to critical systems or protected data.

The Corporation IT manager stated that some forms of information security awareness documentation were available in the new hire package and on new computer account request and Virtual Private Network (VPN) access request forms, but acknowledged that a more formal security

awareness training program could be incorporated, including annual refresher training for employees with access to critical systems or protected data.

Failure to provide employees with information security awareness training increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

### **Recommendation 11**

We recommend that the Corporation develop and implement an information security awareness training program for all employees with access to critical systems or protected data.

### **Campus Response**

We concur. The Corporation will implement an information security awareness training program for all employees with access to critical systems or protected data.

Completion: July 31, 2009

## **PROTECTED DATA ASSESSMENT**

The Corporation did not perform a periodic assessment and inventory of protected information residing on its systems.

The Corporation had not conducted a detailed assessment of protected information residing on auxiliary systems, and the protected information was not formally inventoried in accordance with the *Cal Poly Information Security Program*.

The *Cal Poly Information Security Program* states that all information should be reviewed and classified according to its use, sensitivity, and importance. All information resources should be categorized and protected according to the requirements set for each classification (high risk, internal, or public). An appropriate level of security should be established for all information processed or maintained by Cal Poly and auxiliary organizations based on the classification of the information.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic assessment and inventory of protected information residing on auxiliary systems.

The Corporation IT manager stated that such an assessment and inventory of protected data had not been considered a high priority because of the Corporation migration to a new enterprise resource planning system, IFAS Financials in May 2003 and IFAS Human Resources/Payroll in January 2004. She further stated that Corporation priorities had been to sustain system stability, security, regulatory compliance, operational requirements, and performance of these new system implementations. She added that, in subsequent years, other high priority projects such as a Business Objects Enterprise reporting tool implementation, and creation of the new entity, Cal Poly Corporation, had risen to top of the IT project list.

Inadequate accountability over information assets, especially those containing personal confidential information or with accessibility to such protected information, increases the risk of loss and inappropriate use of auxiliary resources, and exposure to information security breaches.

### **Recommendation 12**

We recommend that the Corporation:

- a. Conduct an assessment and inventory of protected information, and ensure that a reassessment is completed, at least annually. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security officers, and individuals permitted access.
- b. Formally classify all Corporation information resources and require protection in accordance with the data classification scheme outlined in the *Cal Poly Information Security Program* (high risk, internal, or public).

### **Campus Response**

We concur.

- a. We have begun conducting an assessment of the current inventory and security of protected information according to the CSU and campus policy.
- b. We have begun formally classifying the information assets according to the CSU and campus data classification standard.

We will conduct annual reviews to ensure compliance with existing CSU and campus policy.

Completion: July 31, 2009

## **SYSTEM BACKUPS**

Daily, weekly, and monthly backups for Corporation systems with protected data were not encrypted when stored locally or when in transit to the University of California, Santa Barbara for off-site disaster recovery purposes.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the encryption of protected data contained on auxiliary systems and backups.

The Corporation IT manager stated that the campus had not considered it necessary to encrypt data backups as the data was always stored and transported securely. She added that the Corporation also considered the risk of not being able to readily locate the encryption key resulting in either a delayed or failed data recovery.

Inadequate security of system backups increases the risk of inappropriate access to protected data and the possible ramifications of required public notifications should backups be lost when unencrypted.

### **Recommendation 13**

We recommend that the Corporation encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

### **Campus Response**

We concur. As of October 20, 2008, we implemented encryption of system backups and continued the secure off-site transfer and storage of backups. This was completed during audit field work.

## **REMOTE SERVER ACCESS**

Remote access to Corporation servers was not always secure.

Telecommunication Network (Telnet), an unsecure remote access protocol that allows users to connect to remote computers and transmits data in clear text, was enabled on the MBS application server to permit remote access by the vendor (through an opened port/firewall pinhole) for performing system updates. In addition, one bookstore employee was permitted to gain remote access to the MBS application server from his home via this Telnet connection.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates securing remote access to auxiliary systems.

The Corporation El Corral Bookstore associate director of operations stated that the vendor must gain prior authorization from him and the Corporation IT network staff in order to access the MBS system. He added that vendor accounts were disabled soon after the work is completed and there was no protected data stored on the MBS application system. The Corporation IT manager stated that the MBS server and the other IT servers were on different subnets, so any risk exposure due to Telnet remote access was localized to the MBS server. She further stated that the current version of the operating system for the MBS did not appear to support secure shell, a more secure remote access protocol.

Failure to properly secure remote access to auxiliary servers increases the risk that an attacker who is able to monitor network traffic could capture sensitive information or authentication credentials and, therefore, gain access to network resources and exploit vulnerabilities that could lead to the loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

#### **Recommendation 14**

We recommend that the Corporation replace Telnet remote access with a more secure remote access protocol (such as secure shell) or the use of a VPN.

#### **Campus Response**

We concur. As of December 15, 2008, we disabled Telnet remote access to the Corporation's MBS and replaced it with VPN access. This item has been completed.

### **WEB APPLICATION SECURITY**

The Corporation did not formally document the evaluation/testing of the quality and security of web applications prior to moving them into production.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that web applications be checked for quality and security vulnerabilities prior to being put into production.

The Corporation IT manager stated that due to scheduling and resource constraints, the Corporation had not been able to formally document the procedures for developing and testing the web applications, but she added that the Corporation IT developers were familiar with the *Open Web Application Security Project* guidelines.

Failure to formally document evaluation and testing of the quality and security of web applications increases the risk that website applications may contain vulnerabilities that could lead to a loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

#### **Recommendation 15**

We recommend that the Corporation formalize procedures to document the evaluation/testing of the quality and security of web applications.

#### **Campus Response**

We concur. We have begun formalizing the procedures for evaluating and testing the web applications according to the CSU and campus policy.

Completion: July 31, 2009

## **CAL POLY HOUSING CORPORATION**

### **FISCAL COMPLIANCE**

The Cal Poly Housing Corporation (Housing) had not developed a reserve policy.

Such a policy should address the following areas:

- ▶ Minimum reserve requirements.
- ▶ Board review of reserve levels.
- ▶ Reserves for working capital and capital replacement.
- ▶ The methodology used for the calculation of reserves.

Education Code §89904(b), §89904.5, and §89905 indicate that reserve planning is necessary.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.9, *Reserves and Net Assets*, states, in part, an auxiliary implement financial standards, which will assure fiscal viability, including proper provision for professional management, adequate working capital, adequate reserve funds for current operations and capital replacements, and adequate provisions for new business requirements.

The Housing managing director stated that he was unaware of the reserve policy requirement.

The absence of reserve planning and analysis increases the risk that the auxiliary will be unable to fund future needs.

#### **Recommendation 16**

We recommend that Housing develop a documented reserve policy to address the allocation of surplus funds/reserves.

#### **Campus Response**

We concur. A reserve policy was developed and it was approved by the board of directors on December 12, 2008.

## SEGREGATION OF DUTIES

Duties and responsibilities over certain purchasing and payables/disbursement functions were not adequately segregated at Housing.

We found that the Housing managing director:

- ▶ Initiated purchases by generating and approving requisitions.
- ▶ Obtained price quotes and negotiated prices with vendors.
- ▶ Agreed purchase terms and selected vendors.
- ▶ Approved vendor invoices.
- ▶ Generated and approved check requests.
- ▶ Signed checks.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.5, *Procurement*, states, in part, that the auxiliary should establish a written internal controls system that provides purchase orders and service contracts are prepared separately from both receiving and shipping, and payables and disbursements.

The Housing managing director stated that the lack of proper segregation of purchasing and payables/disbursement duties was due to staffing constraints.

Inadequate segregation of duties increases the risk that errors and irregularities will not be detected in a timely manner.

### **Recommendation 17**

We recommend that Housing properly segregate certain purchasing and payables/disbursement functions or institute mitigating procedures approved by the campus CFO.

### **Campus Response**

We concur. The referenced purchasing and payables/disbursement functions have been segregated. The managing director no longer generates requisitions or check requests. The managing director no longer signs manual checks unless he is the second signatory for checks over \$25,000. The same procedure will apply to checks electronically signed once the necessary resolutions and paperwork are completed in March 2009.

**ASSOCIATED STUDENTS, INCORPORATED OF**  
**CALIFORNIA POLYTECHNIC STATE UNIVERSITY AT SAN LUIS OBISPO**

**FACILITIES AGREEMENTS**

Certain lease agreements between the Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo (ASI) and the campus expired.

We found that:

- ▶ The lease agreement between the campus and ASI for the Cal Poly Recreation Center expired on June 30, 2006.
- ▶ The lease agreement between the campus and ASI for the sports complex expired on June 30, 2006.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that facility lease arrangements be supported by current, written agreements.

The ASI executive director stated that the lease agreements in question were designed to automatically extend after the expiration of the initial term. He further stated that new agreements had not been executed due to expansion and renovation projects that would require substantive changes in existing terms and the parties elected to wait until such time as the terms could be clearly determined due to the material change in operational needs of the facilities.

The absence of current, written facilities lease agreements increases the risk of misunderstandings and miscommunication regarding rights and responsibilities.

**Recommendation 18**

We recommend that ASI execute current facilities lease agreements with the campus.

**Campus Response**

We concur. The university and ASI will execute new lease agreements for the two facility leases that were in holdover status.

Completion: July 31, 2009

## PROPERTY AND EQUIPMENT

The annual ASI property reconciliation for fiscal year 2007/08 was not signed and dated by the preparer and reviewer to evidence timely completion and independent review.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should reconcile physical inventories to the general ledger on a timely basis with review by management.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient documentation of timely preparation and independent review of property reconciliations.

The ASI executive director stated that the property reconciliation was completed by the appropriate ASI staff according to current practices, but the current procedures did not require signatures to evidence completion of the reconciliation process.

Failure to sufficiently document property reconciliations increases the risk that errors and irregularities will not be timely detected and accountability will not be maintained.

### **Recommendation 19**

We recommend that ASI ensure that property reconciliations are signed and dated by the preparer and reviewer.

### **Campus Response**

We concur. ASI will implement procedures to ensure that property reconciliations are signed and dated by the preparer and reviewer.

Completion: July 31, 2009

## INFORMATION TECHNOLOGY

### PASSWORD SECURITY

Password security parameters were not always adequate for ASI systems.

The following Active Directory (AD) centralized authentication password security parameters were set outside of leading security standards:

- ▶ Maximum password age: 365 days (for all accounts, including IT administrators).
- ▶ Minimum password age: zero days.
- ▶ Enforced password history: two or three passwords remembered (varied by groups).

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates strong password parameters.

The ASI IT coordinator stated that campus-established parameters had been used for setting up the AD password structure.

Insufficient password parameters increase the risk of unauthorized access to auxiliary systems and confidential data.

#### **Recommendation 20**

We recommend that ASI reassess its security requirements and set effective password security controls for its computer systems, especially for IT administrator accounts with privileged access to systems.

#### **Campus Response**

We concur. ASI will reassess security requirements and change password requirements to provide increased security. IT administrator accounts will be given a higher level of scrutiny to address the sensitivity of the positions.

Completion: July 31, 2009

## **COMPUTER ROOM SECURITY**

There was no fire extinguisher in the ASI server room.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that appropriate fire equipment be maintained within the premises of server/data centers at all times.

The ASI IT coordinator stated that the fire extinguisher that was originally located in the server room was removed by facilities staff for recharging and testing and had not been returned as of the time of this review.

Failure to maintain an appropriate fire extinguisher in the server room increases the risk of unsuccessful containment of a fire, which may expose employees to dangerous conditions and may result in the loss of critical systems.

### **Recommendation 21**

We recommend that ASI maintain an operable class C (for electrical equipment) fire extinguisher in the server room at all times.

### **Campus Response**

We concur. ASI has changed the policy regarding fire extinguisher testing and recharging. When a fire extinguisher is being recharged, an equivalent extinguisher will be located in the IT server room.

Completion: July 31, 2009

## **USER ACCESS REVIEWS**

The ASI did not perform a periodic documented management review of user access privileges within all systems and applications containing protected data.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates a periodic documented review of user access privileges within all systems and applications containing protected data.

The ASI IT coordinator stated that a review of user access was being performed by ASI IT staff, but was not documented or delegated to other operational ASI managers and supervisors.

Failure to periodically perform a documented review of user access to systems containing protected data increases the risk of inappropriate access.

### **Recommendation 22**

We recommend that ASI conduct periodic documented management reviews of user access to systems containing protected data, at least annually.

### **Campus Response**

We concur. ASI will conduct and document periodic reviews of user access to systems containing protected data. The review will be conducted on an annual basis at a minimum.

Completion: July 31, 2009

## **PROTECTED DATA ASSESSMENT**

The ASI did not perform a periodic assessment and inventory of protected information residing on its systems.

The ASI had not conducted a detailed assessment of protected information residing on auxiliary systems, and the protected information was not formally inventoried in accordance with the *Cal Poly Information Security Program*.

The *Cal Poly Information Security Program* states that all information should be reviewed and classified according to its use, sensitivity, and importance. All information resources should be categorized and protected according to the requirements set for each classification (high risk, internal, or public). An appropriate level of security should be established for all information processed or maintained by Cal Poly and auxiliary organization based on the classification of the information.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic assessment and inventory of protected information residing on auxiliary systems.

The ASI IT coordinator stated that an assessment of the protected data based on the Cal Poly Information Security Plan had been conducted several years ago, but documentation of the assessment was not retained.

Inadequate accountability over information assets, especially those containing personal confidential information or with accessibility to such protected information, increases the risk of loss and inappropriate use of auxiliary resources, and exposure to information security breaches.

### **Recommendation 23**

We recommend that ASI:

- a. Conduct an assessment and inventory of protected information, and ensure that reassessment is completed, at least annually. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security officers, and individuals permitted access.
- b. Formally classify all ASI information resources and require protection in accordance with the data classification scheme outlined in the Cal Poly Information Security Plan (high risk, internal, or public).

### **Campus Response**

We concur. ASI will conduct an assessment and inventory of protected information in accordance with the Cal Poly Information Security Plan. The evaluation will be documented, and the process will be performed on an annual basis at a minimum.

Completion: July 31, 2009

## **WEB APPLICATION SECURITY**

The ASI did not formally document the evaluation/testing of the quality and security of web applications prior to moving them into production.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that web applications be checked for quality and security vulnerabilities prior to being put into production.

The ASI IT coordinator stated that procedures were in place for evaluating and testing software applications; however, the procedures were not formally documented.

Failure to formally document evaluation and testing of the quality and security of web applications increases the risk that website applications may contain vulnerabilities that could lead to a loss of protected confidential information, and the execution of malicious programs on the server that could disable additional network resources.

#### **Recommendation 24**

We recommend that ASI formalize procedures to document the evaluation/testing of the quality and security of web applications.

#### **Campus Response**

We concur. ASI will document the security procedures followed when evaluating and/or testing web applications. These procedures will be reviewed on an annual basis at a minimum.

Completion: July 31, 2009

---

## **APPENDIX A: PERSONNEL CONTACTED**

### **Name**

### **Title**

#### **CAMPUS**

Warren J. Baker	President
Lawrence Kelley	Vice President of Administration and Finance
Lorlie Leetham	Director of Fiscal Services
Rick Ramirez	Associate Vice President of Finance
Terry Vahey	Information Security Officer and Director, Technology Services

#### **CALIFORNIA POLYTECHNIC STATE UNIVERSITY FOUNDATION**

Jesselle Miura	Financial Analyst
Craig Nelson	Director of Cal Poly Fund and Advancement Services
Lisa Rockwell-Harpster	Trust Administrator
Linda Stark	Matching Gifts Coordinator
Bob Stets	Chief Financial Officer
Ron Weaver	Investment Administrator

#### **CAL POLY CORPORATION**

Kelly Ayler	Cashier
David Bains	Applications Development Supervisor
Cindy Boone	Payroll Supervisor
Karen Brown	Accounting Manager
Michele Bullock	Customer Service Assistant
Janet Carlstrom	Customer Service Manager, El Corral Bookstore
Frank Cawley	Director, El Corral Bookstore
Lori Cordova	Accounting Manager
Alan Cushman	Associate Director, Campus Dining
Philip Davis	Associate Director of Operations, El Corral Bookstore
Dustin DeBrum	Manager, Educational Web Services
Tammy Farrell	Financial Accounting Coordinator, El Corral Bookstore
Wendy Forrester	Senior Financial Analyst
Maurie Higginbotham	Accounting Specialist
Pat Johnstone	Network System Analyst
Debbie Kirschenmann	General Accounting Clerk
Tim Maxwell	Database Administrator
Melissa Mullen	Manager, Sponsored Programs
Bonnie Murphy	Executive Director
Gayle Nakano	Grant Analyst
Eumi Sprague	Information Technology (IT) Manager
Melissa Swanson	Purchasing Manager, Campus Dining
Rosa Taliaferro	Accounts Receivable Supervisor
Linda Teeple	Accounts Payable Supervisor
Dale Texter	Chief Financial Officer
Mariann Van Pelt	Accounting Project Manager
Thomas Welton	Director, Campus Dining
Joanne Williams	Director, Human Resources

Laura Wunsch Senior Accountant/Analyst

**CAL POLY HOUSING CORPORATION**

Jim Reinhart Managing Director  
Mariann Van Pelt Accounting Project Manager, Cal Poly Corporation

**ASSOCIATED STUDENTS, INCORPORATED OF  
CALIFORNIA POLYTECHNIC STATE UNIVERSITY AT SAN LUIS OBISPO**

Dawn Annoni	Human Resources Technician
Carol Brizendine	Human Resources Coordinator
Dwayne Brummett	Director of Business Services
Celia Chen	Cash Control Assistant
Nancy Clark	Outdoor Recreation Coordinator
Anthony Colvard	IT Coordinator
Darren Connor	Assistant Director, ASI Programs
Steve Garcia	Facility Operations Coordinator
Tonya Iverson	Director, Children's Programs
Rick Johnson	Executive Director
Marcy Maloney	Director, ASI Programs
Gina Murtha	Accounting Coordinator
Daryl Okada	IT Programmer
Nancy Owens	Accounting Technician
Kay Pasillas	Administrative Assistant
Jennifer Von der Lohe	Accounting Technician

## **STATEMENT OF INTERNAL CONTROLS**

### **A. INTRODUCTION**

Internal accounting and related operational controls established by the State of California, the California State University Board of Trustees, and the Office of the Chancellor are evaluated by the University Auditor, in compliance with professional standards for the conduct of internal audits, to determine if an adequate system of internal control exists and is effective for the purposes intended. Any deficiencies observed are brought to the attention of appropriate management for corrective action.

### **B. INTERNAL CONTROL DEFINITION**

Internal control, in the broad sense, includes controls that may be characterized as either accounting or operational as follows:

#### **1. Internal Accounting Controls**

Internal accounting controls comprise the plan of organization and all methods and procedures that are concerned mainly with, and relate directly to, the safeguarding of assets and the reliability of financial records. They generally include such controls as the systems of authorization and approval, separation of duties concerned with recordkeeping and accounting reports from those concerned with operations or asset custody, physical controls over assets, and personnel of a quality commensurate with responsibilities.

#### **2. Operational Controls**

Operational controls comprise the plan of organization and all methods and procedures that are concerned mainly with operational efficiency and adherence to managerial policies and usually relate only indirectly to the financial records.

### **C. INTERNAL CONTROL OBJECTIVES**

The objective of internal accounting and related operational control is to provide reasonable, but not absolute, assurance as to the safeguarding of assets against loss from unauthorized use or disposition, and the reliability of financial records for preparing financial statements and maintaining accountability for assets. The concept of reasonable assurance recognizes that the cost of a system of internal accounting and operational control should not exceed the benefits derived and also recognizes that the evaluation of these factors necessarily requires estimates and judgment by management.

#### **D. INTERNAL CONTROL SYSTEMS LIMITATIONS**

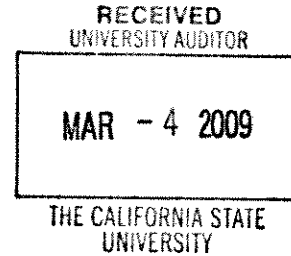
There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal accounting and related operational control. In the performance of most control procedures, errors can result from misunderstanding of instruction, mistakes of judgment, carelessness, or other personal factors. Control procedures whose effectiveness depends upon segregation of duties can be circumvented by collusion. Similarly, control procedures can be circumvented intentionally by management with respect to the executing and recording of transactions. Moreover, projection of any evaluation of internal accounting and operational control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions and that the degree of compliance with the procedures may deteriorate. It is with these understandings that internal audit reports are presented to management for review and use.



California Polytechnic State University  
San Luis Obispo, CA 93407  
Administration & Finance Division  
(805) 756-2171 • Fax (805) 756-7560

27 February 2009

Mr. Larry Mandel  
University Auditor  
Office of the University Auditor  
The California State University  
401 Golden Shore  
Long Beach, CA 90802-4275



Subject: Campus Response to Recommendations of Audit Report Number 08-51,  
Auxiliary Organizations at California Polytechnic State University, San Luis  
Obispo

Dear Larry:

Enclosed in reply to your 06 February 2009 letter to President Baker, are Cal Poly's responses to the auxiliary organizations audit report (Audit Report No. 08-51). The responses are submitted to you for review and for acceptance by the Chancellor. The responses include a corrective action plan and time frame for completion. For any recommended procedures that have been implemented and are in the process of being documented, our responses utilized a standard completion date of not more than 90-days after publication of the final audit report.

Please direct questions to Rick Ramirez, Associate Vice President for Finance, at 805-756-2091 (rramirez@calpoly.edu).

Sincerely,

Lawrence Kelley  
Vice President for Administration & Finance

cc: W. Baker, R. Ramirez

**AUXILIARY ORGANIZATIONS**

**CALIFORNIA POLYTECHNIC STATE UNIVERSITY,  
SAN LUIS OBISPO**

**Audit Report 08-51**

**CAMPUS**

**FEES, REVENUES, AND RECEIVABLES**

**Recommendation 1**

We recommend that the campus improve the matching gifts policy to ensure that a secondary eligibility review is documented prior to the deposit of matching funds to a specifically directed recipient.

**Campus Response**

We concur. Senior University Advancement Services staff are now conducting a secondary review of all matching gifts prior to the deposit of matching funds. This item is completed

Completion: Documentation will be provided within 90 days of publication of the final audit report.

## CAL POLY CORPORATION

### OPERATIONAL COMPLIANCE

#### **Recommendation 2**

We recommend that the Corporation develop policies and procedures to address the management and/or control of waste, spoilage, and shrinkage related to dining and bookstore operations.

#### **Campus Response**

We concur. We will write new procedures to address how the amount for shrinkage is determined, reviewed, and adjusted as part of dining and bookstore annual inventory processes.

Completion: 31 July 2009

### SEGREGATION OF DUTIES

#### **Recommendation 3**

We recommend that the Corporation restrict the campus dining purchasing manager's access to the Eatec dining services system or institute mitigating procedures approved by the campus CFO.

#### **Campus Response**

We concur. Corporation management will restrict the campus dining purchasing manager's access to enter purchase orders and receiving data into the Eatec system and will enhance existing procedures to limit the risk of errors and irregularities.

Completion: 31 July 2009

### FEES, REVENUES, AND RECEIVABLES

#### **Recommendation 4**

We recommend that the Corporation ensure that reconciliations between the general ledger accounting system and the bookstore cashiering system and the MBS be signed and dated by the preparer and reviewer.

#### **Campus Response**

We concur. Effective February 1, 2009 we implemented a procedure that requires staff preparing and reviewing reconciliations to sign and date these documents.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

## **PURCHASING AND ACCOUNTS PAYABLE**

### **Recommendation 5**

We recommend that the Corporation reiterate to staff existing cash disbursement policies and procedures regarding sufficient and appropriate supporting documentation, and timeliness of payment.

### **Campus Response**

We concur. By February 28, 2009 we will complete a review of existing policy and procedures with accounts payable staff to ensure cash disbursement documentation is complete and vendor payments are made timely.

Completion: Documentation will be provided within 90 days of publication of the final audit report

## **PROPERTY AND EQUIPMENT**

### **Recommendation 6**

We recommend that the Corporation:

- a. Ensure that all assets are tagged.
- b. Maintain accurate records of the location and disposal of all assets.

### **Campus Response**

We concur. Corporation receiving procedures will be revised to ensure all equipment is tagged and inventoried by location.

Completion: 31 October 2009.

## **AUXILIARY PROGRAMS**

### **Recommendation 7**

With reference to the description of EO 919 cited above, we recommend that the Corporation and the campus:

- a. Work together to ensure compliance with EO 919, determine if any assets reflected in the Corporation financial statements contain state funds, and move any identified state funds to campus accounts.

b. Certify that none of the following specific and similar monies reside in Corporation accounts:

- Gifts to the university, its units and programs.
- Contracts and grants awarded to the university.
- Fees for continuing education courses provided by the university.
- Fees for university events, workshops, conferences, institutes, special projects, and programs.
- Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
- Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
- Student fees and other general fees pursuant to the CSU student fee policy.
- Monies held by the Corporation via contract with the campus.

c. Provide supporting documentation to evidence the content and review of custodial trust accounts and the reason for the determination made.

#### **Campus Response**

We concur that State funds should not be held by auxiliary organizations. The Corporation and the University will conduct a review to determine if any State funds reside in Corporation accounts and will transfer any State funds to the University.

Completion: 31 December 2009.

## **INFORMATION TECHNOLOGY**

### **PASSWORD SECURITY**

#### **Recommendation 8**

We recommend that the Corporation reassess its security requirements and set effective password security controls and time-out settings for its computer systems.

#### **Campus Response**

We concur. As of October 20, 2008 we implemented enhanced password security controls by modifying the UNIX account "Password History Depth" to the maximum allowed value of 10. At the advice of the Audit Manager we left the "Minimum time between password changes" as "zero weeks", as it offers better security over "one week" (the other option). This item was completed during audit field work.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

## **UNIQUE USER IDS**

### **Recommendation 9**

We recommend that the Corporation assign unique user account IDs to all users accessing and recording transactions in the MCS.

### **Campus Response**

We concur. As of November 1, 2008, we assigned unique user IDs and we provided training and a procedural manual to all cashiers accessing and recording transactions in the Micros Cashiering System installed at the Corporation dining venues. This item has been completed.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

## **USER ACCESS REVIEWS**

### **Recommendation 10**

We recommend that the Corporation conduct periodic documented management reviews of user access to systems containing protected data, at least annually.

### **Campus Response**

We concur. We will formalize the procedure for reviewing user access privileges within all systems and applications containing protected data. We will document the annual management review of such information in accordance with the CSU and campus policy.

Completion: 31 July 2009.

## **INFORMATION SECURITY TRAINING**

### **Recommendation 11**

We recommend that the Corporation develop and implement an information security awareness training program for all employees with access to critical systems or protected data.

### **Campus Response**

We concur. The Corporation will implement an information security awareness training program for all employees with access to critical systems or protected data.

Completion: 31 July 2009.

## PROTECTED DATA ASSESSMENT

### Recommendation 12

We recommend that the Corporation:

- a. Conduct an assessment and inventory of protected information, and ensure that a reassessment is completed, at least annually. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security officers, and individuals permitted access.
- b. Formally classify all Corporation information resources and require protection in accordance with the data classification scheme outlined in the *Cal Poly Information Security Program* (high risk, internal, or public).

### Campus Response

We concur.

- a. We have begun conducting an assessment of the current inventory and security of protected information according to the CSU and campus policy.
- b. We have begun formally classifying the information asset according to the CSU and campus Data Classification Standard.

We will conduct annual reviews to ensure compliance with existing CSU and campus policy.

Completion: 31 July 2009.

## SYSTEM BACKUPS

### Recommendation 13

We recommend that the Corporation encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

### Campus Response

We concur. As of October 20, 2008 we implemented encryption of system backups and continued the secure off-site transfer and storage of backups. This was completed during audit field work.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

## REMOTE SERVER ACCESS

### Recommendation 14

We recommend that the Corporation replace Telnet remote access with a more secure remote access protocol (such as secure shell) or the use of a VPN.

### Campus Response

We concur. As of December 15, 2008 we disabled Telnet remote access to the Corporation's MBS (Missouri Bookstore System) and replaced it with VPN access. This item has been completed.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

## WEB APPLICATION SECURITY

### Recommendation 15

We recommend that the Corporation formalize procedures to document the evaluation/testing of the quality and security of web applications.

### Campus Response

We concur. We have begun formalizing the procedures for evaluating and testing the web applications according to the CSU and campus policy.

Completion: 31 July 2009.

**CAL POLY HOUSING CORPORATION**

**FISCAL COMPLIANCE**

**Recommendation 16**

We recommend that Housing develop a documented reserve policy to address the allocation of surplus funds/reserves.

**Campus Response**

A reserve policy was developed and it was approved by the Board of Directors on December 12, 2008.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

**SEGREGATION OF DUTIES**

**Recommendation 17**

We recommend that Housing properly segregate certain purchasing and payables/disbursement functions or institute mitigating procedures approved by the campus CFO.

**Campus Response**

The referenced purchasing and payables/disbursement functions have been segregated. The Managing Director no longer generates requisitions or check requests. The Managing Director no longer signs manual checks unless he is the second signatory for checks over \$25,000. The same procedure will apply to checks electronically signed once the necessary resolutions and paperwork are completed in March 2009.

Completion: Documentation will be provided within 90 days of publication of the final audit report.

**ASSOCIATED STUDENTS, INCORPORATED OF**  
**CALIFORNIA POLYTECHNIC STATE UNIVERSITY AT SAN LUIS OBISPO**

**FACILITIES AGREEMENTS**

**Recommendation 18**

We recommend that ASI execute current facilities lease agreements with the campus.

**Campus Response**

We concur. The University and ASI will execute new lease agreements for the two facility leases that were in holdover status.

Completion: 31 July 2009.

**PROPERTY AND EQUIPMENT**

**Recommendation 19**

We recommend that ASI ensure that property reconciliations are signed and dated by the preparer and reviewer.

**Campus Response**

We concur. ASI will implement procedures to ensure that property reconciliations are signed and dated by the preparer and reviewer.

Completion: 31 July 2009.

**INFORMATION TECHNOLOGY**

**PASSWORD SECURITY**

**Recommendation 20**

We recommend that ASI reassess its security requirements and set effective password security controls for its computer systems, especially for IT administrator accounts with privileged access to systems.

### **Campus Response**

We concur. ASI will reassess security requirements and change password requirements to provide increased security. IT administrator accounts will be given a higher level of scrutiny to address the sensitivity of the positions.

Completion: 31 July 2009

## **COMPUTER ROOM SECURITY**

### **Recommendation 21**

We recommend that ASI maintain an operable class C (for electrical equipment) fire extinguisher in the server room at all times.

### **Campus Response**

We concur. ASI has changed the policy regarding fire extinguisher testing and recharging. When a Fire extinguisher is being recharged, an equivalent extinguisher will be located in the IT server room.

Completion: 31 July 2009

## **USER ACCESS REVIEWS**

### **Recommendation 22**

We recommend that ASI conduct periodic documented management reviews of user access to systems containing protected data, at least annually.

### **Campus Response**

We concur. ASI will conduct and document periodic reviews of user access to systems containing protected data. The review will be conducted on an annual basis at a minimum.

Completion: 31 July 2009

## **PROTECTED DATA ASSESSMENT**

### **Recommendation 23**

We recommend that ASI:

- a. Conduct an assessment and inventory of protected information, and ensure that reassessment is completed, at least annually. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security officers, and individuals permitted access.

- b. Formally classify all ASI information resources and require protection in accordance with the data classification scheme outlined in the *Cal Poly Information Security Plan* (high risk, internal, or public).

**Campus Response**

We concur. ASI will conduct an assessment and inventory of protected information in accordance with the Cal Poly Information Security Plan. The evaluation will be documented and the process will be performed on an annual basis at a minimum.

Completion: 31 July 2009

**WEB APPLICATION SECURITY**

**Recommendation 24**

We recommend that ASI formalize procedures to document the evaluation/testing of the quality and security of web applications.

**Campus Response**

We concur. ASI will document the security procedures followed when evaluating and/or testing web applications. These procedures will be reviewed on an annual basis at a minimum.

Completion: 31 July 2009

  
**THE CALIFORNIA STATE UNIVERSITY**  
 OFFICE OF THE CHANCELLOR

BAKERSFIELD

March 20, 2009

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

DOMINGUEZ HILLS

TO: Mr. Larry Mandel  
University Auditor

EAST BAY

FROM: Charles B. Reed  
Chancellor

FRESNO

FULLERTON

HUMBOLDT

SUBJECT: Draft Final Audit Report 08-51 on *Auxiliary Organizations*,  
California Polytechnic State University, San Luis Obispo

LONG BEACH

LOS ANGELES

In response to your memorandum of March 20, 2009, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, California Polytechnic State University, San Luis Obispo.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

Enclosure

SACRAMENTO

cc: Dr. Warren J. Baker, President

SAN BERNARDINO

Mr. Lawrence R. Kelley, Vice President, Administration and Finance

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS