DATA CENTER OPERATIONS

CALIFORNIA STATE POLYTECHNIC UNIVERSITY,
POMONA

Audit Report 12-34
October 24, 2012

Members, Committee on Audit

Henry Mendoza, Chair
William Hauck, Vice Chair
Lupe C. Garcia  Steven M. Glazer
Hugo N. Morales  Glen O. Toney

Staff

University Auditor: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditor: Dane MacDonald

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
# CONTENTS

Executive Summary ................................................................................................................................. 1

Introduction ................................................................................................................................................... 3
  Background ........................................................................................................................................... 3
  Purpose ............................................................................................................................................... 5
  Scope and Methodology ......................................................................................................................... 6

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Physical Security ........................................................................................................................................... 7
  Background Checks ............................................................................................................................... 7
  Physical Access .................................................................................................................................... 7
  Security Systems .................................................................................................................................. 8

Fire Protection and Environmental Controls ............................................................................................ 9
  Fire Protection ...................................................................................................................................... 9
  Environmental Controls ....................................................................................................................... 10

Emergency Preparedness and Training ..................................................................................................... 11

Operations, Change Control, and Help Desk ............................................................................................ 12
  Data Backup ....................................................................................................................................... 12
  Change Controls ................................................................................................................................. 13
APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Campus Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

CEU College of Extended University
CSU California State University
FISMA Financial Integrity and State Manager’s Accountability Act
FPM Facilities Planning and Management
I&IT Instructional and Information Technology
ICSUAM Integrated California State University Administrative Manual
MDF Main Distribution Frame
MIS Management Information Systems
OUA Office of the University Auditor
SAM State Administrative Manual
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor (OUA) during the last quarter of 2011, the Board of Trustees, at its January 2012 meeting, directed that Data Center Operations be reviewed. The OUA had previously reviewed some aspects of Data Center Operations in the 2008 and 2009 audits of Information Security and the 2010 and 2011 audits of IT Disaster Recovery Planning. The OUA also reviewed Data Center Operations in the biennial Financial Integrity and State Manager’s Accountability Act (FISMA) audits, the last of which was performed on campus in 2006.

We visited the California State Polytechnic University, Pomona campus from June 11, 2012, through July 12, 2012, and audited the procedures in effect at that time.

Our study and evaluation revealed certain conditions that, in our opinion, could result in significant risk exposures if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: physical security; fire protection and environmental controls; emergency preparedness and training; and operations, change control, and help desk. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, except for the effect of the weaknesses described above, the operational and administrative controls over data center operations in effect as of July 12, 2012, taken as a whole, were sufficient to meet the objectives stated in the “Purpose” section of this report.

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.

Our audit did not examine all controls over data center operations but was designed to assess management controls, increase awareness of the topic, and assess regulatory compliance for significant data center operations categories that are prevalent in the California State University environment.

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

PHYSICAL SECURITY [7]

Background checks were not performed on all employees who had physical access to campus data centers. In addition, campus data centers were not always equipped with an electronic security system to track and monitor personnel entering and exiting the facilities. Further, data center security systems were not adequate to detect or prevent unauthorized entry. Specifically, some data centers did not have a security alarm and/or video camera motion detector.
EXECUTIVE SUMMARY

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [9]

Fire protection measures at campus data centers were not sufficient to detect or suppress fires. For example, some data centers did not have an automatic fire suppression system. Additionally, campus data centers did not always have adequate environmental monitoring systems; specifically, some data centers did not have a water sensor.

EMERGENCY PREPAREDNESS AND TRAINING [11]

Emergency power generators capable of sustaining computer operations in the event of a power outage were not installed at all data processing facilities.

OPERATIONS, CHANGE CONTROL, AND HELP DESK [12]

Backup tapes were not always maintained off-site, and change control procedures had not been developed and implemented for all campus data centers.
INTRODUCTION

BACKGROUND

Integrated California State University Administrative Manual (ICSUAM) §8000.0, Information Security Policy, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding the security and protection of data center operations. It provides direction for managing and protecting the confidentiality, integrity, and availability of California State University (CSU) information assets and defines the organizational scope of information security throughout the system. Specifically, the policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

ICSUAM §8000.0 further states that it is the collective responsibility of all users to ensure the confidentiality of information that the CSU must protect from unauthorized access; the integrity and availability of information stored on or processed by CSU information systems; and compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection.

The policy applies to all campuses; central and departmentally managed campus information assets; all users employed by campuses or any other person with access to campus information assets; all categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic); and information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

ICSUAM §8080 states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas include data centers and other locations on the campus where information assets containing protected data are stored. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets that access protected data located in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. Campuses must review and document physical access rights to campus limited-access areas annually.

State Administrative Manual (SAM) §5330 states that physical security practices prevent unauthorized physical access, damage, and interruption to an agency’s assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take the appropriate physical security measures to provide for: management control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by agency staff and outsiders; prevention, detection, and suppression of fires; and prevention, detection, and minimization of water damage and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

SAM §5335 states that agencies are responsible for the management and operation of their information processing facilities. The security program should identify and document the appropriate practices to
ensure the integrity and security of the agency’s information assets. SAM §5335 references International Standards Organization 17799 Section 9, Physical and Environmental Security, and National Institute of Standards and Technology Special Publication 800-12 (Chapter 15), along with other standards and guidance criteria.

Historically, data center operations were reviewed by the CSU Office of the University Auditor (OUA) as part of cyclical audits based on the Financial Integrity and State Manager’s Accountability Act (FISMA) of 1983, passed by the California Legislature and detailed in Government Code §13400 through §13407. Beginning in calendar year 2010, cyclical FISMA audits were reevaluated and discontinued due to a change in the OUA audit risk assessment methodology. Using the new procedure, the OUA worked with CSU campus executive management to identify high-risk areas on each campus. Data Center Operations was selected as a high-risk area to review in 2012.
INTRODUCTION

PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of data center operations; determine the adequacy of controls over the related processes; and ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, management committees, and documented policies and procedures.
- Data processing facilities employ physical security safeguards for achieving and maintaining appropriate protection of organizational assets.
- Data processing facilities contain adequate fire suppression provisions and employ controls that help maintain a proper operating environment.
- Handling procedures for backup media ensure that the movement and storage of tapes is controlled and accountable.
- Formal event reporting and escalation procedures are in place for job scheduling.
- Change management procedures are sufficient to ensure that modifications to the systems or network are authorized.
- Management review of help desk activities ensures a proactive approach toward determining whether there is a systemic cause to problems reported.
SCOPE AND METHODOLOGY

The proposed scope of the audit as presented in Attachment A, Audit Agenda Item 2 of the January 24 and 25, 2012, meeting of the Committee on Audit stated that Data Center Operations would include review and compliance with Trustee policy, federal and state directives, and campus policies and procedures; physical security provisions; environmental controls; processing and scheduling controls; backup and recovery processes; and emergency preparations.

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 operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the administrative, compliance, operational, and technical controls over the campus data center, network rooms, and personnel operations. Specifically, we reviewed and tested:

- Data center policies and procedures.
- Computer operations organizational structure and management framework.
- Physical security over data processing facilities.
- Fire prevention and environmental controls.
- Emergency preparedness and training.
- Storage and handling of backup media.
- Job scheduling.
- Change management.
- Help desk support.

Our testing and methodology was designed to provide a managerial-level review of key data processing practices over data center operations. Our review did not examine all categories of computer operations; selected IT processes not related to the data center or related data processing facilities were excluded from the scope of the review. Our testing approach was designed to provide a view of the security and controls used to protect only key computing and business processes.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

PHYSICAL SECURITY

BACKGROUND CHECKS

Background checks were not performed on all employees who had physical access to campus data centers.

Integrated California State University Administrative Manual (ICSUAM) §8030, Personnel Information Security, dated April 19, 2010, states that campuses must develop procedures to conduct background checks on positions involving access to level one information assets as defined in the California State University (CSU) Data Classification Standard.

The associate vice president of human resources services stated that the campus began requiring background checks for all new hires after the policy date, but did not consider it a requirement to obtain background checks for employees hired prior to the change in policy.

Failure to screen and perform background checks on personnel who have access to sensitive data increases the risk of potential mishandling and inappropriate disclosure of sensitive data.

Recommendation 1

We recommend that the campus perform background checks on all employees who have physical access to campus data centers.

Campus Response

We concur. The human resources office at the chancellor’s office is updating the background check policy, which will require checks to be performed on all new hires. The policy update will also require employees assigned to sensitive positions to complete the appropriate background checks. Since the policy has not been finalized, the campus will encounter significant collective bargaining issues should it implement background checks ahead of the policy update. It is our objective to implement all applicable aspects of the background check policy when it is issued by the chancellor’s office for all campuses.

Timeline: June 2013

PHYSICAL ACCESS

Campus data centers were not always equipped with an electronic security system to track and monitor personnel entering and exiting the facilities.

We reviewed eight data centers and building distribution frame rooms and found that three did not have an electronic security system.
ICSUAM §8080, Physical Security, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are stored.

State Administrative Manual (SAM) §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for control of physical access to information assets by agency staff and outsiders.

The information security officer stated that the use of key lock systems to protect data rooms in the areas cited was considered adequate to restrict physical access.

Failure to provide an electronic security system increases the risk that unauthorized personnel will have access to information assets, and that the campus will not have the capability to track the date and time of personnel entering and exiting the rooms.

**Recommendation 2**

We recommend that the campus install an electronic security system to track and monitor personnel entering and exiting the facilities in all data centers.

**Campus Response**

We concur. The campus will consolidate the operations of the satellite data centers into the instructional and information technology (I&IT) data center. Access to the I&IT data center is controlled by a proximity card access system that is managed by the campus police. Access to the I&IT data center is limited to personnel whose equipment is collocated or personnel who support or maintain the systems housed in the I&IT data center. Access to the I&IT data center is reviewed on a quarterly basis.

The plan to consolidate data centers on campus will be developed by January 2013, and all satellite data centers will be closed and equipment will be moved into the I&IT data center by June 2013.

**SECURITY SYSTEMS**

Data center security systems were not adequate to detect or prevent unauthorized entry.

We reviewed eight data centers and found that:

- Four did not have a security alarm system and/or a video camera.
- Three had unsecured windows or entry points that could allow for unauthorized access.

ICSUAM §8080, Physical Security, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include
data centers and other locations on the campus where information assets containing protected data are stored.

SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for control of physical access to information assets by agency staff and outsiders.

The information security officer stated that the campus chose to accept the risk of not installing security alarms and video cameras in all the data centers and not closing off all windows or other potential entry points, and focused attention on other, higher-priority security initiatives.

Failure to detect and prevent unauthorized entry to data centers increases the risk of security breaches and theft of computing equipment.

**Recommendation 3**

We recommend that the campus:

a. Install security alarm systems and video cameras in all data centers.
b. Secure all windows and entry points to the data centers.

**Campus Response**

We concur. The campus will consolidate the operations of the satellite data centers into the I&IT data center. The campus also plans to secure all windows and entry points to the data centers as part of the I&IT data center facility upgrade plan.

The plan to complete data center infrastructure upgrades will be developed by February 2013; infrastructure improvements to secure windows and entry points will be complete by February 1, 2013; and additional alarm and security video camera installations will be complete by April 2013.

**FIRE PROTECTION AND ENVIRONMENTAL CONTROLS**

**FIRE PROTECTION**

Fire protection measures at campus data centers were not sufficient to detect or suppress fires.

We reviewed eight data centers and found that:

- Five did not have an automatic fire suppression system.
- One did not have a fire extinguisher.
- One did not have a smoke detector.
SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for prevention, detection, and suppression of fires.

The information security officer stated that fire protection measures were not consistently in place because data center management is highly decentralized on the campus and standards regarding what constitutes adequate fire suppression for a data center had not been developed.

Failure to install automatic fire suppression systems, fire extinguishers, and smoke detectors in data centers increases the risk that information assets will be damaged during disasters or emergencies.

**Recommendation 4**

We recommend that the campus install an automatic fire suppression system, a fire extinguisher, and a smoke detector in each data center.

**Campus Response**

We concur. The campus will consolidate the operations of the satellite data centers into the I&IT data center. The I&IT campus data center is protected by automatic fire suppression and has additional environmental controls to detect threats from fire, water, or changes in temperature.

Timeline: June 2013

**ENVIRONMENTAL CONTROLS**

Campus data centers did not always have adequate environmental monitoring systems.

We reviewed eight data centers and found that:

- Four did not have a water sensor.
- Four did not have a temperature and environmental monitoring device.

SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for prevention, detection, and minimization of water damage.

The information security officer stated that environmental monitoring controls were not consistently in place because data center management is highly decentralized on the campus and standards regarding what constitutes adequate environmental controls had not been developed.

Failure to detect and prevent flooding and other environmental changes in the data center room can result in damaged information assets.
**Recommendation 5**

We recommend that the campus install water sensors and temperature and environmental monitoring devices in each campus data center.

**Campus Response**

We concur. The campus will consolidate the operations of the satellite data centers into the I&IT data center. The I&IT data center has multiple sensors and controls to maintain temperature within a specific range to allow the equipment housed in the data center to perform optimally. The I&IT data center also has environmental monitoring devices.

Timeline: June 2013

**EMERGENCY PREPAREDNESS AND TRAINING**

Emergency power generators capable of sustaining computer operations in the event of a power outage were not installed at all data processing facilities.

Specifically, we found that the data center in the engineering department did not have a backup generator, and a business impact analysis had not been performed to determine whether it was necessary.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states that each campus must ensure that information assets can, in case of a catastrophic event, continue to operate and be appropriately accessible to users.

SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for prevention, detection, and minimization of loss or disruption of operational capabilities due to electrical power fluctuations or failure.

The information security officer stated that the college’s disaster recovery plan noted that the need for generators to sustain the engineering data center in the event of a power outage was not critical.

The lack of backup generators capable of sustaining computer operations increases the risk that the campus could lose the ability to provide data processing services in the event of a power outage, which could disrupt campus operations.

**Recommendation 6**

We recommend that the campus perform a business impact analysis for the engineering department data center to determine whether a backup generator is necessary.
Campus Response

We concur. The campus will consolidate the operations of the satellite data centers into the I&IT data center. A backup generator to support the engineering department data center will not be required.

Timeline: June 2013

OPERATIONS, CHANGE CONTROL, AND HELP DESK

DATA BACKUP

Backup tapes were not always maintained off-site.

We reviewed eight data centers, and two did not maintain backup tapes off-site.

ICSUAM §8085, Business Continuity and Disaster Recovery, dated April 19, 2010, states that each campus must ensure that information assets can, in case of a catastrophic event, continue to operate and be appropriately accessible to users.

The information security officer stated that staff at the two data centers cited were unaware that they could make use of the Iron Mountain off-site tape contract to store their tapes, and the campus had not implemented processes to store all data center backup information off-site due to budget constraints.

Failure to store backup data tapes off-site increases the risk of losing data in the event of a disaster, which could disrupt campus operations.

Recommendation 7

We recommend that the campus store all backup tapes at an off-site location.

Campus Response

We concur. The campus will consolidate the operations of the satellite data centers into the I&IT data center. All back-up tapes will be stored at an off-campus facility.

Timeline: June 2013
CHANGE CONTROLS

Change control procedures had not been developed and implemented for all campus data centers.

We found that one of the eight data centers did not have a formal process for addressing problems and managing changes to departmental systems.

ICSUAM §8055 Change Control, dated April 19, 2010, states that changes to information technology systems, network resources, and applications need to be appropriately managed to minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted. Campuses must establish and document a process to manage changes to campus information assets containing level 1 or level 2 data, as defined in the CSU Data Classification Standard.

The information security officer stated that the formal change control process was not in place because periodic vulnerability scans were performed on that data center’s servers, which he considered sufficient to minimize the risk of introducing vulnerabilities.

Failure to develop a formal process for addressing problems and managing changes to campus information assets increases the possibility of security risk to campus systems.

Recommendation 8

We recommend that the campus develop and implement change control procedures at all campus data centers.

Campus Response

We concur. The campus will consolidate the operations of the satellite data centers into the I&IT data center. Assets housed in the I&IT data center will follow the campus information technology change control procedures.

Timeline: June 2013
# APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>J. Michael Ortiz</td>
<td>President</td>
</tr>
<tr>
<td>Albert Arboleda</td>
<td>Information Security Officer, Instructional and Information Technology (I&amp;IT) Information Security</td>
</tr>
<tr>
<td>Mark Bailey</td>
<td>Department Engineer, Electrical and Computer Engineering Department</td>
</tr>
<tr>
<td>Edwin Barnes</td>
<td>Vice President, Administrative Affairs</td>
</tr>
<tr>
<td>Cathy Bates</td>
<td>Director, Student Affairs Applications and Technology Solutions/Student Affairs Information and Technology Services</td>
</tr>
<tr>
<td>Jarod Beekman</td>
<td>Associate Director of Networking and Telecommunications, I&amp;IT Systems</td>
</tr>
<tr>
<td>Eric Bellman</td>
<td>Manager Systems Operations, Administrative Affairs Information Systems</td>
</tr>
<tr>
<td>Joseph Bustamante</td>
<td>Information Systems Analyst, Management Information Systems (MIS) Foundation</td>
</tr>
<tr>
<td>David Drivdahl</td>
<td>Interim Director of System Administration, I&amp;IT Systems</td>
</tr>
<tr>
<td>Joseph Galdonik</td>
<td>Systems Support Technician, College of Engineering</td>
</tr>
<tr>
<td>Kathy Harper</td>
<td>Assistant to the Vice President, Finance and Administrative Services</td>
</tr>
<tr>
<td>Hovig Krikorian</td>
<td>Associate Systems Analyst, College of the Extended University</td>
</tr>
<tr>
<td>Gabriel Kuri</td>
<td>Senior Network Engineer, I&amp;IT Systems</td>
</tr>
<tr>
<td>Christopher Laasch</td>
<td>Information Technology Administrative, Student Affairs Information and Technology Services</td>
</tr>
<tr>
<td>Darwin Labordo</td>
<td>Associate Vice President, Finance and Administrative Services</td>
</tr>
<tr>
<td>Cecilia Lenasdotter</td>
<td>Information Systems Analyst, MIS Foundation</td>
</tr>
<tr>
<td>Whitney Lopez</td>
<td>Administrative Support Coordinator, I&amp;IT Systems</td>
</tr>
<tr>
<td>Walter Marquez</td>
<td>Director, Facilities Administrative and Energy Services</td>
</tr>
<tr>
<td>Mary Martinez</td>
<td>Payroll Manager, Human Resource Services</td>
</tr>
<tr>
<td>Debbi McFall</td>
<td>Emergency Service Coordinator, University Police</td>
</tr>
<tr>
<td>John McGuthry</td>
<td>Chief Information Officer, I&amp;IT</td>
</tr>
<tr>
<td>Mark Miller</td>
<td>Director, Facilities Management and Capital Projects</td>
</tr>
<tr>
<td>Kevin Morningstar</td>
<td>Executive Director, Student Affairs Information and Technology Services</td>
</tr>
<tr>
<td>Denton Mosier</td>
<td>Executive Director Technical Support, I&amp;IT Support</td>
</tr>
<tr>
<td>Son Phan</td>
<td>Senior Systems Analyst, College of Engineering</td>
</tr>
<tr>
<td>Sharon Reiter</td>
<td>Associate Vice President, Human Resource Services</td>
</tr>
<tr>
<td>James Schneider</td>
<td>Network Analyst, I&amp;IT Systems</td>
</tr>
<tr>
<td>Randall Townsend</td>
<td>Management Information Systems Manager, MIS Foundation</td>
</tr>
<tr>
<td>Mark VanDusen</td>
<td>Systems Support Technician, College of Engineering</td>
</tr>
<tr>
<td>Joice Xiong</td>
<td>Director of Internal Audits, Administrative Affairs</td>
</tr>
<tr>
<td>Glendy Yeh</td>
<td>Executive Director, Administrative Affairs Information Systems</td>
</tr>
</tbody>
</table>
November 27, 2012

Mr. Larry Mandel, University Auditor
Office of the Auditor
The California State University
400 Golden Shore, Suite 210
Long Beach, CA 90802

Dear Mr. Mandel:

Subject: Campus Response – Data Center Operations 12-34

Enclosed is California State Polytechnic University, Pomona’s campus response to the Data Center Operations Audit 12-34. We appreciate the effort you and your staff have made to indicate areas where our procedures or internal controls could be strengthened. We will take the necessary actions to address the report’s recommendations.

Please direct questions concerning the response to Darwin Labordo, Associate Vice President of Finance and Administrative Services and Associate Chief Financial Officer at 909-869-2008 or dlabordo@csupomona.edu.

Sincerely,

[Signature]

Edwin A. Barnes, III, Vice President
Administrative Affairs

Cc: J. Michael Ortiz, President
Albert Arboleda, Information Security Officer, I&IT Information Security
Darwin Labordo, Associate Vice President, Finance & Administrative Services
John W. McGuthy, Chief Information Officer, Instructional & Information Technology
Sharon Reiter, Associate Vice President, Human Resource Services
Joice Xiong, University Auditor

Enclosure
DATA CENTER OPERATIONS
CALIFORNIA STATE POLYTECHNIC UNIVERSITY,
POMONA
Audit Report 12-34

PHYSICAL SECURITY

BACKGROUND CHECKS

Recommendation 1

We recommend that the campus perform background checks on all employees who have physical access to campus data centers.

Campus Response

We concur.

The HR office at Chancellor’s Office is updating the background check policy which will require checks to be performed on all new hires. The policy update will also require employees assigned to sensitive positions to complete the appropriate background checks. Since the policy has not been finalized, the campus will encounter significant collective bargaining issues should it implement background checks ahead of the policy update. It is our objective to implement all applicable aspects of the background check policy when it is issued by Chancellor’s Office for all campuses.

Timeline: June 2013

PHYSICAL ACCESS

Recommendation 2

We recommend that the campus install an electronic security system to track and monitor personnel entering and exiting the facilities in all data centers.

Campus Response

We concur.

The campus will consolidate the operations of the satellite data centers into the I&IT data center. Access to the I&IT data center is controlled by a proximity card access system that is managed by the campus police. Access to the I&IT data center is limited to personnel whose equipment is collocated or personnel who support or maintain the systems housed in the I&IT data center. Access to the I&IT data center is reviewed on a quarterly basis.
• Plan to consolidate data centers on campus will be developed by January 2013
• All satellite data centers will be closed and equipment will be moved into the I&IT data center by June 2013

Timeline: June 2013

SECURITY SYSTEMS

Recommendation 3

We recommend that the campus:

a. Install security alarm systems and video cameras in all data centers.
b. Secure all windows and entry points to the data centers.

Campus Response

We concur.

The campus will consolidate the operations of the satellite data centers into the I&IT data center. The campus also plans to secure all windows and entry points to the data centers as part of the I&IT data center facility upgrade plan.

• Plan to complete data center infrastructure upgrades developed by February 2013
• Infrastructure improvements to secure windows and entry points complete by February 1, 2013
• Additional alarm and security video camera installations complete by April 2013

Timeline: April 2013

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

FIRE PROTECTION

Recommendation 4

We recommend that the campus install an automatic fire suppression system, a fire extinguisher, and a smoke detector in each data center.

Campus Response

We concur.

The campus will consolidate the operations of the satellite data centers into the I&IT data center. The I&IT campus data center is protected by automatic fire suppression and has additional environmental controls to detect threats from fire, water or changes in temperature.

Timeline: June 2013
ENVIRONMENTAL CONTROLS

Recommendation 5

We recommend that the campus install water sensors and temperature and environmental monitoring devices in each campus data center.

Campus Response

We concur.

The campus will consolidate the operations of the satellite data centers into the I&IT data center. The I&IT data center has multiple sensors and controls to maintain temperature within a specific range to allow the equipment housed in the data center to perform optimally. The I&IT data center also has environmental monitoring devices.

Timeline: June 2013

EMERGENCY PREPAREDNESS AND TRAINING

Recommendation 6

We recommend that the campus perform a business impact analysis for the engineering department data center to determine whether a backup generator is necessary.

Campus Response

We concur.

The campus will consolidate the operations of the satellite data centers into the I&IT data center. A backup generator to support the engineering department data center will not be required.

Timeline: June 2013

OPERATIONS, CHANGE CONTROL, AND HELP DESK

DATA BACKUP

Recommendation 7

We recommend that the campus store all backup tapes at an off-site location.

Campus Response

We concur.
The campus will consolidate the operations of the satellite data centers into the I&IT data center. All back-up tapes will be stored at an off-campus facility.

Timeline: June 2013

CHANGE CONTROLS

Recommendation 8

We recommend that the campus develop and implement change control procedures at all campus data centers.

Campus Response

We concur.

The campus will consolidate the operations of the satellite data centers into the I&IT data center. Assets housed in the I&IT data center will follow the campus information technology change control procedures.

Timeline: June 2013
January 2, 2013

MEMORANDUM

TO: Mr. Larry Mandel
University Auditor

FROM: Timothy P. White
Chancellor

SUBJECT: Draft Final Report 12-34 on Data Center Operations, California State Polytechnic University, Pomona

In response to your memorandum of January 2, 2013, I accept the response as submitted with the draft final report on Data Center Operations, California State Polytechnic University, Pomona.

TPW/amd