## CONTENTS

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

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

### OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

Physical Security ........................................................................................................................................... 7
  Background Checks .................................................................................................................................. 7
  Data Center Access .................................................................................................................................. 7
  Facility Access Control and Monitoring ................................................................................................... 9
  Alarm Systems ........................................................................................................................................ 10

Fire Protection and Environmental Controls .............................................................................................. 11
  Fire Protection ......................................................................................................................................... 11
  Satellite Data Center Controls ................................................................................................................ 12

Emergency Preparedness and Training ....................................................................................................... 13
  Emergency Power ................................................................................................................................... 13
  Procedures and Training ......................................................................................................................... 13
## APPENDICES

- **APPENDIX A**: Personnel Contacted
- **APPENDIX B**: Management Response
- **APPENDIX C**: Chancellor’s Acceptance

## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATS</td>
<td>Academic Technology Services</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CO</td>
<td>Office of the Chancellor</td>
</tr>
<tr>
<td>CSU</td>
<td>California State University</td>
</tr>
<tr>
<td>F&amp;A</td>
<td>Finance and Administration</td>
</tr>
<tr>
<td>FISMA</td>
<td>Financial Integrity and State Manager’s Accountability Act</td>
</tr>
<tr>
<td>ICSUAM</td>
<td>Integrated California State University Administrative Manual</td>
</tr>
<tr>
<td>I&amp;IT</td>
<td>Instructional and Information Technology</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information Systems</td>
</tr>
<tr>
<td>OUA</td>
<td>Office of the University Auditor</td>
</tr>
<tr>
<td>SAM</td>
<td>State Administrative Manual</td>
</tr>
<tr>
<td>T&amp;C</td>
<td>Technology and Communication</td>
</tr>
</tbody>
</table>
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 campuses in 2009.

We visited six campuses from February 20, 2012, through September 7, 2012, and audited the procedures in effect at that time. Campus-specific findings and recommendations have been discussed and reported individually.

In our opinion, due to the effect of the weaknesses described below, the fiscal, operational and administrative controls for data center operations as of September 7, 2012, taken as a whole, were not sufficient to meet the objectives stated in the “Purpose” section of this report. Areas of major concern include: physical security, fire protection and environmental controls, and emergency preparedness and training.

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 the campus data centers or systems that contain sensitive data. In addition, access to campus data center rooms was not always limited to those individuals whose responsibilities required access. Further, restriction of physical access to data rooms and monitoring of personnel who entered and exited those rooms needed improvement. For example, the doors to campus data centers and network main distribution frame rooms were not always equipped with electronic access control systems to track and monitor personnel entering and exiting the facilities, and most campuses did not have procedures to regularly monitor access reports from existing electronic key card systems. Also, data and computing facilities were not always adequately protected to detect unauthorized physical access.
EXECUTIVE SUMMARY

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [11]

The campuses had not provided adequate fire detection and suppression controls to ensure that facilities were protected, and satellite data centers operated by campus departments did not always have adequate fire suppression or environmental monitoring systems.

EMERGENCY PREPAREDNESS AND TRAINING [13]

Emergency power generators capable of sustaining computer operations in the event of a power outage were not in use at all campus data centers. In addition, data center emergency preparedness and training required improvement. Specifically, campuses did not always have documented data center emergency operations procedures, and data center personnel were not always trained in the operation of the fire suppression system and the use of fire extinguishers.
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.
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.

During the course of the audit, we visited six campuses: Channel Islands, Chico, Dominguez Hills, Long Beach, East Bay, and Pomona. We interviewed campus personnel and audited procedures in effect at the time of the audit.
PHYSICAL SECURITY

BACKGROUND CHECKS

Background checks were not performed on all employees who had physical access to the campus data centers or systems that contain sensitive data.

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.

Campus management stated various reasons for background checks not being performed, including lack of awareness that checks were required and the understanding that the Office of the Chancellor (CO) was developing a systemwide policy on background checks to address compliance with applicable laws, policies, and bargaining unit agreements, which the campuses planned to adopt.

Failure to 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 CO reiterate to the campuses that background checks are required for all employees who have physical access to the campus data centers or systems that contain sensitive data.

Management Response

Management concurs. The CO will remind the campuses that background checks are required per ICSUAM §8030, and that background checks should be conducted in compliance with CSU Human Resources and Labor Relations policy. This notification will take place by September 30, 2013.

DATA CENTER ACCESS

Access to campus data center rooms was not always limited to those individuals whose responsibilities required access.

Specifically, we noted that:

- Several individuals were incorrectly granted access, and others with access no longer required it or had been terminated.
Individuals from various campus departments, such as custodial, facilities, and police services, had been granted data center access, even though their current responsibilities did not warrant it. Most individuals with questionable access were given master keys rather than electronic key cards that would have allowed management to track and monitor when they entered and exited the room.

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. 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 that are 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.

Campus management stated various reasons for the inappropriate physical access and the lack of policies and procedures over monitoring, including a lack of guidance on the access roles of campus support personnel and failure to properly consider access via physical master keys.

Inadequate physical security over information technology assets and sensitive data information increases the risk that unauthorized personnel will have access to information assets.

**Recommendation 2**

We recommend that the CO:

a. Ensure that campuses limit access to campus data center rooms to those individuals whose responsibilities require access.

b. Remind the campuses that they are required to periodically review and validate physical access rights to server rooms and data centers housing systems containing level 1 sensitive data.

c. Ensure that the campus CIOs submit an annual certification of compliance with physical security standards and procedures to include an attestation that physical security rights have been reviewed and are appropriate.

**Management Response**

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8080. The CO will also notify the campuses that they are required to submit an annual certification that they are in compliance with the related physical security standards and procedures. This notification will take place not later than September 30, 2013.
FACILITY ACCESS CONTROL AND MONITORING

Restriction of physical access to data rooms and monitoring of personnel who entered and exited those rooms needed improvement.

Specifically, we found that:

- The doors to campus data centers and network main distribution frame (MDF) rooms housing systems with level 1 data were not always equipped with electronic access control systems to track and monitor personnel entering and exiting the facilities.

- Most campuses did not have procedures to regularly monitor access reports from existing electronic key card systems.

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 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.

Campus management stated that electronic locks had not been placed in all facilities due to the high cost of installation. Management further stated that they were unaware of the need to monitor door access logs, and that the MDFs were not routinely inspected due to oversight.

Failure to adequately restrict access and monitor personnel who enter and exit the data center and adequately secure network devices could increase the risk of unauthorized or inappropriate activity occurring without detection.

**Recommendation 3**

We recommend that the CO ensure that campuses:

a. Equip data centers and MDF rooms housing systems with level 1 data with electronic access control systems to track and monitor personnel entering and exiting the facilities.

b. Establish procedures to regularly monitor access reports from electronic key card systems.

c. Ensure that the campus CIOs submit an annual certification that physical security controls are equipped on all data centers housing level 1 data.
Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8080 and §5330.

Campuses will be advised to: a) equip data centers and MDF rooms housing systems with level 1 data with electronic access control systems, or relocate systems with level 1 data to facilities that are so equipped; and b) establish procedures to regularly monitor access reports from the access control systems.

The CO will also notify the campuses that they are required to submit an annual certification that they are in compliance with the related physical security standards and procedures. This notification will take place not later than September 30, 2013.

ALARM SYSTEMS

Data and computing facilities were not always adequately protected to detect unauthorized physical access.

Specifically, we noted that unattended data centers, server rooms, and network MDF rooms housing systems with level 1 data did not always have security alarm systems installed to detect entry.

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. 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 that are 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.

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 campus chief information officers (CIO) stated that alarms had not been installed in data centers because the rooms were located in buildings that were secured after hours. They further stated that security alarms had not been placed in the MDF rooms due to installation and monitoring costs.

Failure to equip computer rooms with security alarm systems increases the risk of security breaches and theft of computing equipment.
Recommendation 4

We recommend that the CO:

a. Remind the campuses that they are required to identify and protect data centers, server rooms, MDF rooms, and any other area housing systems containing level 1 or level 2 sensitive data.

b. Ensure that the campus CIOs submits an annual certification of compliance with systemwide physical security policies.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8080 and §5330. The CO will also notify the campuses that they are required to submit an annual certification that they are in compliance with systemwide physical security policies. This notification will take place not later than September 30, 2013.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

FIRE PROTECTION

The campuses had not provided adequate fire detection and suppression controls to ensure that facilities were protected.

Specifically, we noted that campus primary data centers did not always have smoke detection systems or automatic fire suppression systems.

SAM §5330 states that physical 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 campus CIOs stated their belief that passing the building fire inspection was confirmation that their data center fire provisions were sufficient.

A lack of smoke detectors and fire suppression equipment in data centers increases the risk that information assets will be damaged during disasters or emergencies.

Recommendation 5

We recommend that the CO validate that the campuses have implemented adequate fire detection and suppression controls to protect primary data centers in the event of fire.
Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §5330. The CO will also ensure that campuses submit an annual certification that they are in compliance with the related physical security and fire safety standards and procedures. This notification will take place not later than September 30, 2013.

SATELLITE DATA CENTER CONTROLS

Satellite data centers operated by campus departments did not always have adequate fire suppression or environmental monitoring systems.

We reviewed several departmental data centers, and we found that they did not always have automatic fire suppression systems, fire extinguishers, smoke detectors, water sensors, and temperature and environmental monitoring devices.

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 campus CIOs stated that fire protection measures and environmental controls were not consistently in place because data center management was highly decentralized, and standards regarding what constitutes adequate fire suppression for a data center had not been developed.

A lack of automatic fire suppression systems, fire extinguishers, smoke detectors, and environmental controls in data centers increases the risk that information assets will be damaged during disasters or emergencies.

Recommendation 6

We recommend that the CO ensure that campuses have provided adequate fire suppression and environmental monitoring systems in satellite data centers, or ensure that the campuses consolidate those facilities into data centers that provide such controls.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §5330. Campuses will be advised to equip satellite data centers housing systems with level 1 data with appropriate fire suppression and environmental monitoring systems, or relocate systems with level 1 data to facilities that provide such controls. This notification will take place not later than September 30, 2013.
EMERGENCY PREPAREDNESS AND TRAINING

EMERGENCY POWER

Emergency power generators capable of sustaining computer operations in the event of a power outage were not in use at all campus data centers.

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 campus CIOs stated that backup power generators had not been purchased or installed due to the extremely high cost.

A 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 7

We recommend that the CO ensure that campuses install emergency power generators capable of sustaining computer operations in the event of a power outage in data center rooms, or move equipment into computing facilities that have backup power.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8085 and §5330. Campuses will be advised to install emergency power generators in satellite data centers housing systems with level 1 data, or relocate systems with level 1 data to facilities with such equipment. This notification will take place not later than September 30, 2013.

PROCEDURES AND TRAINING

Data center emergency preparedness and training required improvement.

We found that:

- Campuses did not always have documented data center emergency operations procedures.
Data center personnel were not always trained in the operation of the fire suppression system and the use of fire extinguishers.

SAM §5355.1 states that disaster recovery plans and other IT procedures should be developed to ensure that critical services and applications are restored as quickly as possible and with minimal loss of data.

The campus CIOs stated that the lack of formal data center emergency operations procedures and the failure to provide fire suppression and safety equipment training to data center personnel were due to oversight.

Inadequate data center emergency systems procedures and training could lead to misunderstandings and confusion in the event of a disaster or emergency.

**Recommendation 8**

We recommend that the CO:

a. Ensure that campuses develop and test data center emergency operations procedures.

b. Issue specific guidance regarding requirements for training data center personnel on fire suppression and safety equipment.

**Management Response**

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §5355.1. Campuses will be advised to develop and test data center emergency operations procedures, paying particular attention to fire and life safety. This notification will take place not later than September 30, 2013.
## APPENDIX A:
PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chancellor’s Office</td>
<td></td>
</tr>
<tr>
<td>Benjamin F. Quillian</td>
<td>Executive Vice Chancellor and Chief Financial Officer</td>
</tr>
<tr>
<td>Bruce Briggs</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Mark Crase</td>
<td>Senior Director, Technology Infrastructure Services</td>
</tr>
<tr>
<td>William Perry</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>Michael Redmond</td>
<td>Senior Director, Chancellor's Office Fiscal Control and Special Initiatives</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>California State University, Channel Islands</td>
<td></td>
</tr>
<tr>
<td>Richard R. Rush</td>
<td>President</td>
</tr>
<tr>
<td>Pamela Abbot-Mouchou</td>
<td>Executive Administrative Assistant, Finance and Administration (F&amp;A)</td>
</tr>
<tr>
<td>Herbert Aquino</td>
<td>Manager of Information Technology Infrastructure, Technology and Communication (T&amp;C)</td>
</tr>
<tr>
<td>Melissa Bergem</td>
<td>Project Coordinator, T&amp;C</td>
</tr>
<tr>
<td>Michael Berman</td>
<td>Vice President, T&amp;C</td>
</tr>
<tr>
<td>Will Brogdon</td>
<td>Student, T&amp;C</td>
</tr>
<tr>
<td>Caroline Doll</td>
<td>Director, F&amp;A</td>
</tr>
<tr>
<td>Diana Enos</td>
<td>Human Resources Manager, F&amp;A</td>
</tr>
<tr>
<td>Liza Ernst</td>
<td>Programs Assistant, Human Resources</td>
</tr>
<tr>
<td>Neal Fisch</td>
<td>Director Application Services, T&amp;C</td>
</tr>
<tr>
<td>Judy Frazier</td>
<td>Budget Analyst, T&amp;C</td>
</tr>
<tr>
<td>Ernesto Gutierrez</td>
<td>Senior Network Analyst, T&amp;C</td>
</tr>
<tr>
<td>Theresa Kocis</td>
<td>Fire Alarm Specialist, Operations</td>
</tr>
<tr>
<td>Kristin Steiner</td>
<td>Administrative Support Coordinator, T&amp;C</td>
</tr>
<tr>
<td>Aaron Lasely</td>
<td>Supervising Locksmith, Operations</td>
</tr>
<tr>
<td>Michael Long</td>
<td>Senior Telecommunications Analyst, T&amp;C</td>
</tr>
<tr>
<td>Nasser Mansour</td>
<td>Database Administrator, T&amp;C</td>
</tr>
<tr>
<td>Peter Mosinskis</td>
<td>Director of Information Technology Strategy, T&amp;C</td>
</tr>
<tr>
<td>Jess Paredes</td>
<td>Operating Systems Analyst, T&amp;C</td>
</tr>
<tr>
<td>Richard Paulson</td>
<td>Supervising Building Service Engineer, Operations</td>
</tr>
<tr>
<td>Anna Pavin</td>
<td>Associate Vice President, Human Resources</td>
</tr>
<tr>
<td>Ysabel Trinidad</td>
<td>Vice President, F&amp;A</td>
</tr>
<tr>
<td>Indy Valencia</td>
<td>Manager User Services, T&amp;C</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>California State University, Chico</td>
<td></td>
</tr>
<tr>
<td>Paul J. Zingg</td>
<td>President</td>
</tr>
<tr>
<td>Sharyn Abernatha</td>
<td>Assistant Vice President for Staff Human Resources</td>
</tr>
<tr>
<td>Scott Claverie</td>
<td>Director of Communications Services</td>
</tr>
<tr>
<td>Lee Cummings</td>
<td>Supervisor, Telecommunication Services</td>
</tr>
<tr>
<td>Amy Gremore</td>
<td>Manager of Employment Services</td>
</tr>
</tbody>
</table>

Data Center Operations/Systemwide/Audit Report 12-30
Page 15
APPENDIX A: PERSONNEL CONTACTED

California State University, Chico (cont.)
Lorraine Hoffman  Vice President for Business and Finance
Ed Hudson  Information Security Officer
Jeni Kitchell  Interim Director of University Budget and Resource Management
Andrea Mox  Manager, Information Technology (IT) Support Services
Mike Murray  Administrative Desktop Management
Dennis Partington  Network Manager
Ray Quinto  Manager, Enterprise Systems
Ryan Richter  Labs and Academic Desktop Management
Jerry Ringel  Director, Computing and Technology Support
Tom Rosenow  Director, Application Development and Technical Support, Enrollment Management
Michael Schilling  Vice Provost for Information Resources and Chief Information Officer
Kevin Weherly  Desktop Support Services

California State University, Dominguez Hills
Willie Hagan  President
Mildred Garcia  President (At time of review)
Mahabub Alam  Network Specialist, Campus Backbone Network
Ron Bergmann  Associate Vice President and Chief Information Officer, IT
Ed Laio  Network Analyst
Danny Lujan  Director of Infrastructure
Mary Ann Rodriquez  Vice President, Administration and Finance
Jonathan Scheffler  Associate Director, Physical Plant
Karen Wall  Associate Vice President, Administration and Finance
Muneca Williams  IT Administrative Support Assistant

California State University, East Bay
Leroy M. Morishita  President
Rich Avila  Director, Server and Network Operations
Lee Breitzman  Lead Operations Specialist, Server Operations
Matt Collins  Director, Application Systems
Chris Da Silva  Network Analyst
Maggie Graney  Director, Compliance and Internal Control
Jim Hodges  Chief of Police
Audrey Katzman  Information Technology Business Manager
Gene Lim  Director, Server Operations Services
David Miller  Maintenance Manager, Facilities Management
Setareh Sarrafan  Director of User Support Services
Borre Ulrichsen  Deputy Chief Information Officer
Brad Wells  Vice President and Chief Financial Officer, Administration and Finance
## California State University, Long Beach

Donald J. Para  
Interim President  
F. King Alexander  
President (At time of review)  
Martha Carey  
Data Center Operator  
Janet Foster  
Associate Vice President, Information Technology Services (ITS)  
Vickie Hamilton  
Director, Human Resources  
Byron Jackson  
Director of Service Management and Operations, ITS  
Craig Kleen  
Assistant Director of Network Services, ITS  
Roman Kochan  
Interim Associate Vice President of Academic Technology Services (ATS) and Dean and Director, University Library  
Steve La  
Director of Network, Telecommunication and Security, ITS  
Michael Markoski  
Director of Data Center and Emergency Management, ITS  
Greg Pascal  
Communications/Information System Manager, University Police  
Cheryl Perkins  
Administrative Services Manager  
Wayne Pierson  
Director of Servers, Systems and Websites, ITS  
Aysu Spruill  
Director of Internal Auditing/Information Security Officer  
Mary Stephens  
Vice President, Administration and Finance  
Ryan Tapp  
Library, Desktop and User Support, ATS  
Don Taylor  
Operating Systems Technical Lead, ITS Servers, Systems and Web

## California State Polytechnic University, Pomona

J. Michael Ortiz  
President  
Albert Arboleda  
Information Security Officer, Instructional and Information Technology (I&IT) Information Security  
Mark Bailey  
Department Engineer, Electrical and Computer Engineering Department  
Edwin Barnes III  
Vice President, Administrative Affairs  
Cathy Bates  
Director, Student Affairs Applications and Technology Solutions/Student Affairs Information and Technology Services  
Jarod Beekman  
Associate Director of Networking and Telecommunications, I&IT Systems  
Eric Bellman  
Manager Systems Operations, Administrative Affairs Information Systems  
Joseph Bustamante  
Information Systems Analyst, Management Information Systems (MIS) Foundation  
David Drivdahl  
Interim Director of System Administration, I&IT Systems  
Joseph Galdonik  
Systems Support Technician, College of Engineering  
Kathy Harper  
Assistant to the Vice President, Finance and Administrative Services  
Hovig Krikorian  
Associate Systems Analyst, College of the Extended University  
Gabriel Kuri  
Senior Network Engineer, I&IT Systems  
Christopher Laasch  
Information Technology Administrative, Student Affairs Information and Technology Services  
Darwin Labordo  
Associate Vice President, Finance and Administrative Services  
Cecilia Lenasdotter  
Information Systems Analyst, MIS Foundation  
Whitney Lopez  
Administrative Support Coordinator, I&IT Systems  
Walter Marquez  
Director, Facilities Administrative and Energy Services
APPENDIX A: PERSONNEL CONTACTED

California State Polytechnic University, Pomona (cont.)
Mary Martinez       Payroll Manager, Human Resource Services
Debbi McFall        Emergency Service Coordinator, University Police
John McGuthry       Chief Information Officer, I&IT
Mark Miller         Director, Facilities Management and Capital Projects
Kevin Morningstar  Executive Director, Student Affairs Information and Technology Services
Denton Mosier       Executive Director Technical Support, I&IT Support
Son Phan            Senior Systems Analyst, College of Engineering
Sharon Reiter       Associate Vice President, Human Resource Services
James Schneider     Network Analyst, I&IT Systems
Randall Townsend   Management Information Systems Manager, MIS Foundation
Mark VanDusen       Systems Support Technician, College of Engineering
Joice Xiong        Director of Internal Audits, Administrative Affairs
Glendy Yeh         Executive Director, Administrative Affairs Information Systems
MEMORANDUM

DATE: July 19, 2013

TO: Larry Mandel
    University Auditor

FROM: Benjamin F. Quillian
      Executive Vice Chancellor and
      Chief Financial Officer

SUBJECT: Audit Report # 12-30 Data Center Operations Audit

In response to the "Incomplete Draft" report dated April 23, 2013, we are providing the enclosed management responses.

Should you have any questions, please feel free to contact us.

BFQ: mpr

Attachment

cc: Bruce Briggs, AVC/CIO Information Technology
    Mark Crase, Chief Technology Officer
    William Perry, Chief Info Management & Security Officer
    Michael Redmond, Sr. Dir. CO Budget and Special Initiatives
DATA CENTER OPERATIONS
SYSTEMWIDE
Audit Report 12-30

PHYSICAL SECURITY

BACKGROUND CHECKS

Recommendation 1

We recommend that the CO reiterate to the campuses that background checks are required for all employees who have physical access to the campus data centers or systems that contain sensitive data.

Management Response

Management concurs. The CO will remind the campuses that background checks are required per ICSUAM §8030, and that background checks should be conducted in compliance with CSU Human Resources and Labor Relations policy. This notification will take place by September 30, 2013.

DATA CENTER ACCESS

Recommendation 2

We recommend that the CO:

a. Ensure that campuses limit access to campus data center rooms to those individuals whose responsibilities require access.

b. Remind the campuses that they are required to periodically review and validate physical access rights to server rooms and data centers housing systems containing level 1 sensitive data.

c. Ensure that the campus CIOs submit an annual certification of compliance with physical security standards and procedures to include an attestation that physical security rights have been reviewed and are appropriate.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8080. The CO will also notify the campuses that they are required to submit an annual certification that they are in compliance with the related physical security standards and procedures. This notification will take place not later than September 30, 2013.
FACILITY ACCESS CONTROL AND MONITORING

Recommendation 3

We recommend that the CO ensure that campuses:

a. Equip data centers and MDF rooms housing systems with level 1 data with electronic access control systems to track and monitor personnel entering and exiting the facilities.

b. Establish procedures to regularly monitor access reports from electronic key card systems.

c. Ensure that the campus CIOs submit an annual certification that physical security controls are equipped on all data centers housing level 1 data.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8080 and §5330.

Campuses will be advised to: a) equip data centers and MDF rooms housing systems with level 1 data, with electronic access control systems or to relocate systems with Level 1 data to facilities that are so equipped; and b) establish procedures to regularly monitor access reports from the access control systems.

The CO will also notify the campuses that they are required to submit an annual certification that they are in compliance with the related physical security standards and procedures. This notification will take place not later than September 30, 2013.

ALARM SYSTEMS

Recommendation 4

We recommend that the CO:

a. Remind the campuses that they are required to identify and protect data centers, server rooms, MDF rooms, and any other area housing systems containing level 1 or level 2 sensitive data.

b. Ensure that the campus CIOs submits an annual certification of compliance with system-wide physical security policies.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8080 and §5330. The CO will also notify the campuses that they are required to submit an annual certification that they are in compliance with system-wide physical security policies. This notification will take place not later than September 30, 2013.
FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

FIRE PROTECTION

Recommendation 5

We recommend that the CO validate that the campuses have implemented adequate fire detection and suppression controls to protect primary data centers in the event of fire.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §5330. The CO will also ensure that campuses submit an annual certification that they are in compliance with the related physical security and fire safety standards and procedures. This notification will take place not later than September 30, 2013.

SATELLITE DATA CENTER CONTROLS

Recommendation 6

We recommend that the CO ensure that campuses have provided adequate fire suppression and environmental monitoring systems in satellite data centers, or ensure that the campuses consolidate those facilities into data centers that provide such controls.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §5330. Campuses will be advised to equip satellite data centers housing systems with level 1 data, with appropriate fire suppression and environmental monitoring systems, or to relocate systems with Level 1 data to facilities that provide such controls. This notification will take place not later than September 30, 2013.

EMERGENCY PREPAREDNESS AND TRAINING

EMERGENCY POWER

Recommendation 7

We recommend that the CO ensure that campuses install emergency power generators capable of sustaining computer operations in the event of a power outage in data center rooms, or move equipment into computing facilities that have backup power.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §8085 and §5330. Campuses will be advised to install emergency power generators in satellite data centers housing systems with level 1 data, or to relocate systems with Level 1 data to facilities with such equipment. This notification will take place not later than September 30, 2013.
PROCEDURES AND TRAINING

Recommendation 8

We recommend that the CO:

a. Ensure that campuses develop and test data center emergency operations procedures.

b. Issue specific guidance regarding requirements for training data center personnel on fire suppression and safety equipment.

Management Response

Management concurs. The CO will remind the campuses of their obligations under ICSUAM §5355.1. Campuses will be advised to develop and test data center emergency operations procedures, paying particular attention to fire and life safety. This notification will take place not later than September 30, 2013.
September 4, 2013

MEMORANDUM

TO: Mr. Larry Mandel
University Auditor

FROM: Timothy P. White
Chancellor

SUBJECT: Draft Final Report 12-30 on *Data Center Operations*, Systemwide

In response to your memorandum of September 4, 2013, I accept the response as submitted with the draft final report on *Data Center Operations*, Systemwide.

TPW/amd