DATA CENTER OPERATIONS

CALIFORNIA STATE UNIVERSITY,
CHANNEL ISLANDS

Audit Report 12-36
November 2, 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 Auditors:  Dane MacDonald and Kim Pham
## CONTENTS

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

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

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

**Policies and Procedures** ................................................................................................................................. 7  

**Physical Security** .......................................................................................................................................... 7  
  Physical Access ........................................................................................................................................... 7  
  Computer Room Labeling ........................................................................................................................... 8  
  Background Checks ................................................................................................................................... 9  
  Data Center Access ................................................................................................................................ 10  
  Physical Access Monitoring ....................................................................................................................... 11  

**Fire Protection and Environmental Controls** .............................................................................................. 12
APPENDICES

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

ABBREVIATIONS

BDF Building Distribution Frame
CSU California State University
F&A Finance and Administration
FISMA Financial Integrity and State Manager’s Accountability Act
ICSUAM Integrated California State University Manual
OPC Operations, Planning and Construction
OUA Office of the University Auditor
SAM State Administrative Manual
T&C Technology and Communication
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 2009.

We visited the California State University, Channel Islands campus from August 13, 2012, through September 7, 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: policies and procedures, physical security, and fire protection and environmental controls. 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 September 7, 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.

POLICIES AND PROCEDURES [7]

The campus had not developed written incident response policies and procedures addressing training, incident reporting, and application of lessons learned from information security incidents.

PHYSICAL SECURITY [7]

The data center and two network rooms contained windows that could allow unauthorized entry. In addition, computer room doors were marked with descriptive labels that could increase the risk of unauthorized entry. Also, background checks were not performed on employees who had physical access...
to the campus data center. Further, administration of data center access needed improvement. For example, the campus did not have policies and procedures to regularly certify the list of individuals with authorized access to the data center, building distribution frame (BDF) rooms, and network rooms, and certain individuals with access to the data center no longer appeared to need it. Additionally, the security methods used to restrict access to the data center did not always allow for tracking and monitoring of individuals who entered and exited the facility.

**FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [12]**

Fire protection measures in the campus BDF rooms and network rooms were not sufficient to adequately detect or suppress fires.
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.
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

POLICIES AND PROCEDURES

The campus had not developed written incident response policies and procedures addressing training, incident reporting, and application of lessons learned from information security incidents.

Integrated California State University Manual (ICSUAM) §8075, Information Security Incident Management, dated April 19, 2010, states that campuses must develop and maintain an information security incident response program that includes processes for investigating, responding to, reporting, and recovering from incidents involving loss, damage, misuse of information assets containing protected data, or improper dissemination of critical or protected data, regardless of the medium in which the breached information is held or transmitted (e.g., physical or electronic). The campus information security incident response plans must be reviewed and documented annually and comply with the California State University (CSU) Information Security Incident Management Standards.

The vice president for technology and communication stated that security incident response policies and procedures had not been finalized due to oversight.

Failure to develop security incident response policies and procedures increases the risk that sensitive information may be compromised, or that security incidents may go unnoticed.

Recommendation 1

We recommend that the campus develop written incident response policies and procedures addressing training, incident reporting, and application of lessons learned from information security incidents.

Campus Response

We agree. The campus will complete and adopt written incident response policies and procedures addressing training, incident reporting, and application of lessons learned from information security incidents.

This will be completed by April 30, 2013.

PHYSICAL SECURITY

PHYSICAL ACCESS

The data center and two network rooms contained windows that could allow unauthorized 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.

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.

The manager of information technology infrastructure stated that the security of the windows had not been improved due to budget constraints and a focus on more pressing issues.

Failure to secure all potential entry points to the data center and network rooms increases the risk of security breaches and theft of computing equipment.

**Recommendation 2**

We recommend that the campus secure all windows into the data center and network rooms.

**Campus Response**

We agree with the recommendation for the data center. The campus will have windows secured in the data center by April 30, 2013. However, because we do not store information assets containing protected data in our network rooms, the campus accepts the risk of windows in network rooms.

**COMPUTER ROOM LABELING**

Computer room doors were marked with descriptive labels that could increase the risk of unauthorized entry.

We found that 14 of 15 computer room doors, including the ones to the data center, building distribution frame (BDF) rooms, and network rooms, were marked with labels reading “data center,” “data closet,” and “data equipment.”

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 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 manager of information technology infrastructure stated that the campus had not removed the descriptive labels on the doors to the data center, BDF rooms, and network rooms due to oversight.
Placing descriptive labels on computer room doors increases the risk of unauthorized access and theft of computing equipment.

**Recommendation 3**

We recommend that the campus remove the descriptive labels on the doors to the data center, BDF rooms, and network rooms.

**Campus Response**

We agree that we should not use the labels “data center,” “data closet,” or “data equipment” on our data center, BDF, and network rooms. However, because the Fire Marshal has directed that every door on campus be labeled, we propose to change the room labels to “Equipment Room.” If this proposal is approved, the campus will have labeling changes completed by June 30, 2013.

**BACKGROUND CHECKS**

Background checks were not performed on employees who had physical access to the campus data center.

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 CSU Data Classification Standard.

The human resources manager for finance and administration stated that background checks had not been performed due to the campus’ understanding that the chancellor’s office was developing a systemwide policy on background checks to address compliance with applicable laws, policies, and bargaining unit agreements that the campus 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 4**

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

**Campus Response**

We agree. The campus is in the process of completing background checks on all non-represented employees who have physical access to the campus data center. This will be completed by March 1, 2013. Background checks will also be conducted on newly hired represented and non-represented employees.
DATA CENTER ACCESS

Administration of data center access needed improvement.

Specifically, we found that:

- Two individuals with access to the data center were employees who had been terminated, and 56 individuals with access no longer appeared to need it.

- One individual whose access should have been limited to only the data center’s co-location area had access to the entire center.

- Thirty-two individuals with access to the BDF and wire rooms no longer appeared to need it.

- The campus did not have policies and procedures to regularly certify the list of individuals with authorized access to the data center, BDF rooms, and network rooms.

ICSUAM §8060, Access Control, dated April 19, 2010, states that access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege. Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked. Additionally, the campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

California State University, Channel Islands Campus Locks and Keys Policy (FA.40.002) states that operations, planning and construction (OPC) is responsible for maintaining a central inventory of campus locks, associated keys, and personnel authorized for access and their issued keys and/or access code(s). Campus departments shall notify OPC of pending employee separation to de-activate access codes, and facilitate return of all keys issued to that individual.

The manager of information technology infrastructure stated that the inappropriate physical access and lack of policies and procedures over monitoring and custody was due to the failure to properly transition into a new security system and discontinue the use of legacy systems.

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


Recommendation 5

We recommend that the campus:

a. Remove access to the data center, BDF rooms, and network rooms from individuals without a demonstrated need.

b. Develop policies and procedures to regularly certify access to the data center, BDF rooms, and network rooms.

Campus Response

We agree. The campus will:

a. Remove access to the data center, BDF rooms, and network rooms from individuals without a demonstrated need.

b. Develop policies and procedures to regularly certify access to the data center, BDF rooms, and network rooms.

These data center access correction measures will be completed by April 30, 2013.

PHYSICAL ACCESS MONITORING

The security methods used to restrict access to the data center did not always allow for tracking and monitoring of the individuals who entered and exited the facility.

We found that four separate security methods were being used to control access to the data center, and of the four, only the electronic card keys were equipped with security mechanisms that allowed for tracking and monitoring of personnel who entered and exited the facility.

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 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 manager of information technology infrastructure stated that individuals continued to use physical keys, magnetic fobs, and the pin pad for access to the data center because the campus had not yet had time to fully migrate to the electronic key card system.
Failure to monitor personnel who enter and exit the data center could increase the risk of unauthorized or inappropriate activity occurring without detection.

**Recommendation 6**

We recommend that the campus ensure that security methods used to restrict access to the data center allow for tracking and monitoring of individuals who enter and exit the facility.

**Campus Response**

We agree. The campus will ensure that security methods are used to restrict access to the data center and that they allow for tracking and monitoring of individuals who enter and exit the facility.

These security methods will be in effect and documented by June 30, 2013.

**FIRE PROTECTION AND ENVIRONMENTAL CONTROLS**

Fire protection measures in the campus BDF rooms and network rooms were not sufficient to adequately detect or suppress fires.

We reviewed 15 BDF and network rooms and found that:

- Five did not have a smoke detector.
- Four did not have sprinklers or a nearby fire extinguisher.

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 manager of information technology infrastructure stated that the failure to improve fire protection measures in the campus BDF rooms and wire rooms was due to oversight.

Failure to install smoke detectors and fire extinguishers increases the risk that information assets will be damaged during disasters or emergencies.

**Recommendation 7**

We recommend that the campus install:

a. A smoke detector in each BDF and network room.

b. Either a sprinkler system or a nearby fire extinguisher for each BDF and network room.
Campus Response

Because the rooms referenced in the recommendation are not used to store sensitive information, and because they have been regularly inspected for safety and approved by the Fire Marshal, the campus accepts the risk of BDF and network rooms that do not contain smoke detectors, sprinklers, and/or fire extinguishers.
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
9 January 2013

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4200

RE: Campus Responses to Recommendations: Audit Report 12-36 –Data Center Operations

Dear Mr. Mandel:

Enclosed is our response to the recommendations found in the Audit Report 12-36 – Data Center Operations at California State University Channel Islands. Upon acceptance of our response, the campus will follow up with your office to provide supporting documentation for each of the recommendations by the anticipated completion dates.

Please note that with respect to Recommendations 2 and 7, the campus has elected to accept risk exposure.

If there are questions or if additional information is necessary, please contact Caroline Doll, Director of Special Projects for Finance and Administration, at caroline.doll@csuci.edu or (805) 437-3232.

Sincerely yours,

Richard R. Rush
President

Enclosure

cc: Ysabel Trinidad
Policies and Procedures

Recommendation 1

We recommend that the campus develop written incident response policies and procedures addressing training, incident reporting, and application of lessons learned from information security incidents.

Campus Response

We agree. The campus will complete and adopt written incident response policies and procedures addressing training, incident reporting, and application of lessons learned from information security incidents.

This will be completed by April 30, 2013.

Physical Security

Physical Access

Recommendation 2

We recommend that the campus secure all windows into the data center and network rooms.

Campus Response

We agree with the recommendation for the data center. The campus will have windows secured in the data center by April 30, 2013. However, because we do not store information assets containing protected data in our network rooms, the campus accepts the risk of windows in network rooms.

Computer Room Labeling

Recommendation 3

We recommend that the campus remove the descriptive labels on the doors to the data center, BDF rooms, and network rooms.
Campus Response

We agree that we should not use the labels “data center,” “data closet,” or “data equipment” on our data center, BDF, and network rooms. However, because the Fire Marshal has directed that every door on campus be labeled, we propose to change the room labels to “Equipment Room.” If this proposal is approved, the campus will have labeling changes completed by June 30, 2013.

BACKGROUND CHECKS

Recommendation 4

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

Campus Response

We agree. The campus is in the process of completing background checks on all non-represented employees who have physical access to the campus data center. This will be completed by March 1, 2013. Background checks will also be conducted on newly hired represented and non-represented employees.

DATA CENTER ACCESS

Recommendation 5

We recommend that the campus:

a. Remove access to the data center, BDF rooms, and network rooms from individuals without a demonstrated need.

b. Develop policies and procedures to regularly certify access to the data center, BDF rooms, and network rooms.

Campus Response

We agree. The campus will:

a. Remove access to the data center, BDF rooms, and network rooms from individuals without a demonstrated need.

b. Develop policies and procedures to regularly certify access to the data center, BDF rooms, and network rooms.

These data center access correction measures will be completed by April 30, 2013.
PHYSICAL ACCESS MONITORING

Recommendation 6

We recommend that the campus ensure that security methods used to restrict access to the data center allow for tracking and monitoring of individuals who enter and exit the facility.

Campus Response

We agree. The campus will ensure that security methods are used to restrict access to the data center and that they allow for tracking and monitoring of individuals who enter and exit the facility.

These security methods will be in effect and documented by June 30, 2013.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

Recommendation 7

We recommend that the campus install:

a. A smoke detector in each BDF and network room.

b. Either a sprinkler system or a nearby fire extinguisher for each BDF and network room.

Campus Response

Because the rooms referenced in the recommendation are not used to store sensitive information, and because they have been regularly inspected for safety and approved by the Fire Marshal, the campus accepts the risk of BDF and network rooms that do not contain smoke detectors, sprinklers, and/or fire extinguishers.
February 15, 2013

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Timothy P. White
       Chancellor

SUBJECT: Draft Final Report 12-36 on Data Center Operations,
         California State University, Channel Islands

In response to your memorandum of February 15, 2013, I accept the response
as submitted with the draft final report on Data Center Operations, California
State University, Channel Islands.

TPW/amd