## CONTENTS

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

Introduction................................................................................................................................................... 3
  Background ............................................................................................................................................... 3
  Purpose ...................................................................................................................................................... 5
  Scope and Methodology ............................................................................................................................ 7

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Business Impact Assessment ........................................................................................................................ 8

Alternate Processing ..................................................................................................................................... 9
  Alternate Processing Facility .................................................................................................................... 9
  Alternate Processing Equipment ............................................................................................................. 10

Backup Procedures ...................................................................................................................................... 11

End-User Coordination and Restoration Procedures .................................................................................. 12

Disaster Recovery Planning ........................................................................................................................ 13
  Written Disaster Recovery Plan .............................................................................................................. 13
  Disaster Recovery Plan Testing .............................................................................................................. 15
APPENDICES

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

ABBREVIATIONS

CSU California State University
EO Executive Order
EOC Emergency Operations Center(s)
FISMA Financial Integrity and State Manager’s Accountability
ICSUAM Integrated California State University Administrative Manual
I&ITS Instructional and Information Technology Systems
ITDR Information Technology Disaster Recovery
SAM State Administrative Manual
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2009, the Board of Trustees, at its January 2010 meeting, directed that Information Technology Disaster Recovery (ITDR) be reviewed. The Office of the University Auditor had previously reviewed ITDR for financial systems in the biennial Financial Integrity and State Manager’s Accountability (FISMA) and Auxiliary Organization audits.

We visited the California State Polytechnic University, Pomona campus from April 19, 2010, through April 29, 2010, and audited the procedures in effect at that time.

Our study and evaluation revealed certain conditions that, in our opinion, would result in significant risk exposures if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: business impact assessment, alternate processing, and disaster recovery plan. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, due to the effect of the weaknesses described above, the operational and administrative controls for ITDR in effect as of April 29, 2010, taken as a whole, were not 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 of these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

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

BUSINESS IMPACT ASSESSMENT [8]

The campus had not completed the business impact assessment portion of the business continuity plan, and target dates for its completion had not been identified. As a result, the campus had not determined the business requirements needed to create a viable ITDR plan.

ALTERNATE PROCESSING [9]

Campus planning for restoration of processing capabilities after a disaster needed improvement. Specifically, campus personnel had an informal plan to relocate to another data processing facility on campus, but the plan had not been documented in writing or shared with the campus community. In addition, the campus had not determined how much equipment it would need to relocate to the alternate facility or confirmed whether the facility could support the additional equipment. Further, the campus had not clearly documented a plan for replacement equipment and/or had not secured a contract with a vendor to ensure that substitute equipment would be available in a timely manner after a disaster.
EXECUTIVE SUMMARY

BACKUP PROCEDURES [11]
Backup tapes for the library system were rotated off-site to the personal residence of an employee.

END-USER COORDINATION AND RESTORATION PROCEDURES [12]
IT recovery expectations had not been clearly communicated to the individual business units.

DISASTER RECOVERY PLANNING [13]
There was no current written plan for the overall recovery of IT services. Recovery strategies had been completed for each of the IT areas, but there was no overarching documented plan that outlined the specific steps that should be followed in a local disaster. Also, the campus had not designed a comprehensive plan to test the recovery plan strategies.
INTRODUCTION

BACKGROUND

Information Technology Disaster Recovery (ITDR) planning is a specific subset of an entity’s business continuity planning process that addresses how the IT resources required to operate critical business functions will be restored in a timely and effective manner following a disaster. ITDR planning requires the interaction of individuals at every level of an organization and a recognition by the organization that, in today’s computer-driven work environment, the loss of data processing capabilities can lead to significant financial loss and non-financial exposures if an organization has not planned properly for such an occurrence.

The ITDR planning process requires the evaluation and consideration of several factors, including:

- Who will coordinate the recovery activities, and which supporting groups will report to that coordinator.
- How business units will be impacted if data processing capabilities are lost.
- Which IT systems are critical to support those business units.
- How systems will be restored in the event of a disaster, whether alternate processing facilities will be necessary, whether backup hardware should be stockpiled, and whether insurance coverage will be needed to cover the costs of recovery activities.
- The kind of training individuals involved with the recovery activities will need to ensure they will be prepared to respond to a disaster in a concise and coordinated manner.
- What incidents have occurred in the past that tested the recovery capabilities of the IT systems, how plans have been modified as a result of the incidents, and what simulated testing is required to refine the effectiveness of the plan.

Because organizational and operational design variances exist between the 23 campuses and the Office of the Chancellor, each campus process must consider many unique factors. Campuses have been directed to prepare ITDR plans for disasters via multiple directives, including, but not limited to, State Administrative Manual (SAM) §5355-5355.2, Executive Order (EO) 1014, and the Integrated California State University Administrative Manual (ICSUAM) §8085.0.

SAM §5355-5355.2 directs state agencies to develop, implement, test, and modify disaster recovery plans, including plans specific to IT assets. SAM §5355 states that agencies must take appropriate steps to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure that essential business functions will continue in the event of a disaster. SAM §5355.1 states that, in developing an ITDR plan, agencies should provide for the continuity of computing operations in support of critical business functions, minimize the need for decision-making during a disaster and subsequent recovery, and plan for the migration of computing resources toward resumption of operational capacity in an expeditious and efficient manner. In preparing such a plan, SAM §5355.1 directs that ongoing testing, analysis, and modification of plan assumptions and activities must occur. SAM §5355.2 states that each
agency must maintain a list of computer applications that are critical to agency operations, information assets required by such applications, and a method by which such applications will be reestablished.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, provides detailed guidance to campuses for creating, implementing, and maintaining a business continuity program that includes an ITDR plan. EO 1014 states that goals, which must be met by such a program, include, but are not limited to:

- Maintaining a program on each campus that ensures the continuity of essential functions or operations following a catastrophic event.
- Establishing recovery goals and objectives for the campus that reflect the needs of the campus and its business units.
- Identifying functions and assets that are essential to the operational continuity needed to support the campus’ mission.
- Recommending recovery strategies based on the circumstances of various events.
- Listing, prioritizing, and establishing recovery time objectives for essential functions, systems, and applications through business impact analyses and risk assessments.
- Establishing and testing alternate data processing capabilities, if deemed necessary.
- Protecting and safeguarding vital database systems and data assets.
- Reviewing, testing, modifying, and validating recovery plans in terms of campus and business unit expectations.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, represents the most recent and specific guidance to campuses in regard to ITDR planning. Simply stated, the policy directs campuses to ensure that information assets can continue to operate or, in a reasonable time frame, be supplancted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster or other emergency event. While the policy itself does not provide detailed operational requirements, it can be surmised that the campuses must consider a multitude of factors such as restart times, backup and recovery procedures, system security (environmental, physical, and logical), and system interdependence and redundancy to ensure a satisfactory level of continued operational capacity.
PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to ITDR planning and to determine the adequacy of controls that ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the audit objective, specific goals included determining whether:

- The administration of the ITDR program incorporates a defined mission, stated goals and objectives, and clear lines of organizational authority and responsibility, and is adequately funded.
- The ITDR plan is reviewed and modified on a regular basis, and modifications reflect the needs of the campus and the business units.
- Adequate system redundancy or alternate processes exist to ensure minimal interruption of critical business services.
- System backups and record retention are sufficient to meet the recovery objectives of the campus.
- Initiatives and investments are underway to improve ITDR planning and maximize ITDR resources; risks specific to the campus have been identified; and policies and procedures are current, comprehensive, and sufficient to support campus ITDR planning.
- An adequate emergency operations center (EOC) exists; sufficient equipment, supplies, and other critical resources are properly provisioned; and the campus is fully prepared for emergencies affecting data processing activities.
- The ITDR plan clearly identifies who has authority and responsibility for emergencies and incidents, and the emergency organization is sufficient to ensure that campus command/incident command techniques provide command and control when emergency incidents occur.
- ITDR resources are available; plans have been updated appropriately; and plans are integrated with the campus business continuity plan.
- Previous incidents were mitigated in a timely manner; lessons learned were evaluated; appropriate after-action reports were prepared; and sufficient plans for mitigation of any such incidents in the future are in place.
- Simulated tests of plan components are routinely scheduled, and after-action reports and modifications are generated.
- The potential outage times expected while executing the ITDR plan have been adequately communicated to and coordinated with the campus community, and emergency communications and operations are adequately coordinated and managed.
The campus business units have taken an active role in determining the prioritization of systems and their recovery time expectations.

Sufficient training has been provided to employees, disaster recovery staff, and building marshals who are expected to execute the ITDR plan, and the finance function has been integrated into the disaster recovery activities.

The ITDR plan is written so that a competent individual or group of individuals who are unfamiliar with the campus’ systems would be able to execute a portion or all of the recovery steps if needed.
SCOPE AND METHODOLOGY

The proposed scope of this audit was presented in Attachment A of Audit Agenda Item 2 during the January 26 and 27, 2010, meeting of the Committee on Audit. The attachment stated that the ITDR audit would include a review of Trustee policy, systemwide directives, campus policies and procedures, the essential functions or operations following a catastrophic event, business impact analysis and risk assessment, business continuity and disaster recovery plans, testing and exercising of plans, plan maintenance, communications, training, and necessary retention of key records.

The scope of this audit is focused on the campus’ ITDR planning specific to a disaster only affecting data processing services.

Our study and evaluation was 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 in effect during fiscal year 2009/10. In instances wherein it was necessary to review annualized data, calendar years 2009 and 2010 were the periods reviewed.

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

- The ITDR planning management organization.
- The ITDR plan for all critical campus data processing activities.
- Disaster recovery plan guidelines, policies, procedures, and recordkeeping.
- The building marshal program, emergency action plans, and campus emergency hotline, as it relates to IT disasters.
- The EOC, emergency equipment, and related emergency supplies applicable to ITDR.
- Coordination with other agencies and vendors, including mutual aid and assistance.
- Funding and budgetary controls for disaster recovery planning activities.
- Communication of the disaster recovery plan.
- Training for emergency activities affecting data processing.
- Evacuation drills and emergency plan testing affecting campus data processing facilities.
- Backup and retention of system data.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

BUSINESS IMPACT ASSESSMENT

Business continuity planning needed improvement.

We noted that the campus had not completed the business impact assessment portion of the business continuity plan, and target dates for its completion had not been identified. As a result, the campus had not determined the business requirements needed to create a viable Information Technology Disaster Recovery (ITDR) plan.

State Administrative Manual (SAM) §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.2 states that each agency must maintain a disaster recovery plan that identifies the systems that are critical to the agency’s operations, the information assets required to operate the systems, and a tested process by which the systems will be restored.

Executive Order (EO) 1014, California State University Business Continuity Plan, dated October 8, 2007, states that the campus must develop plans to protect all critical data assets to ensure minimum data loss and continued business functionality in the event of a disaster.

Integrated California State University Administrative Manual (ICSUAM) §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The business continuity coordinator stated that the campus was progressing sequentially through the business units and that it planned to complete business continuity information collection toward the end of the fall quarter of 2010. The director of instructional & information technology systems (I&ITS) stated that the ITDR plans were based on their estimation of a reasonable recovery time that would not generate extensive costs, but that defined business recovery time frames would help to refine the recovery alternatives and validate the existing plan.

Failure to properly determine the business impact of a loss of data processing services prevents the campus from determining how long business operations could continue before suffering severe degradation of business services or excessive monetary loss, and prevents the campus from providing realistic expectations for the recovery planning of data processing services.

Recommendation 1

We recommend that the campus complete the business impact assessment and evaluate the ITDR plan against the business requirements for the recovery of data processing services.
Campus Response

We concur. The campus is working toward the completion of the business impact assessment portion of the business continuity plan. The findings of the business impact assessment will be used in the assignment of recovery priorities among business processes and the applications and infrastructures that support them. The findings of the business impact assessment will also be used to validate the recovery time objectives of the existing ITDR plans.

Expected completion date for business impact assessments: December 17, 2010

Expected completion date for using findings of the business impact assessments to validate the recovery time objectives of the ITDR plan: March 23, 2011

ALTERNATE PROCESSING

ALTERNATE PROCESSING FACILITY

Campus planning for restoration of processing capabilities after a disaster needed improvement.

Specifically, we found that:

- Campus personnel had an informal plan to relocate to another data processing facility on campus, but the plan had not been documented in writing or shared with the campus community.

- The campus had not determined how much equipment it would need to relocate to the alternate facility or confirmed whether the facility could support the additional equipment.

SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.2 states that each agency must maintain a disaster recovery plan that identifies the systems that are critical to the agency’s operations, the information assets required to operate the systems, and a tested process by which the systems will be restored.

EO 1014, California State University Business Continuity Plan, dated October 8, 2007, states that the campus must develop plans to protect all critical data assets to ensure minimum data loss and continued business functionality in the event of a disaster.

ICSUAM §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The I&ITS director stated that recovery alternatives had been included in the previous disaster recovery plan and that current plans would be documented once the business recovery requirements were defined. He also stated that most of the equipment was readily available in the commercial
retail market and that contracting with vendors to provide replacement equipment had been considered.

Failure to properly develop alternative processing capabilities can result in both financial and non-financial losses to the campus and the California State University (CSU) and can result in unexpected delays in the recovery of data processing services.

**Recommendation 2**

We recommend that the campus:

a. Formalize and document the plan to relocate to another data processing facility on campus and share this information with the campus community.

b. Determine the equipment that would need to be located to the alternate facility and validate that the facility can accommodate the additional equipment.

**Campus Response**

We concur.

a. The ITDR plan will address the relocation and resumption of critical IT services provided by the primary data processing facility to an alternate location on and off-campus.

b. The plan for the alternate data processing facility will address all equipment needs and consider strategies to reduce the disruption of critical IT services.

Timeline: March 23, 2011

**ALTERNATE PROCESSING EQUIPMENT**

The campus had not clearly documented a plan for replacement equipment and/or had not secured a contract with a vendor to ensure that substitute equipment would be available in a timely manner after a disaster.

We found that the campus had compiled a list of the data processing equipment housed in its two computing facilities, but there were no specific steps for acquiring replacement equipment in an emergency situation.

SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.2 states that each agency must maintain a disaster recovery plan that identifies the systems that are critical to the agency’s operations, the information assets required to operate the systems, and a tested process by which the systems will be restored.
The I&ITS director stated that most of the equipment used was readily available in the commercial retail market and that the campus had considered contracting with vendors to provide replacement equipment.

Failure to properly develop alternative processing capabilities can result in both financial and non-financial losses to the campus and the CSU and can result in unexpected delays in the recovery of data processing services.

**Recommendation 3**

We recommend that the campus document the specific equipment that it would need to replace immediately after a disaster, as well as a strategy for acquiring such equipment in time to meet the business recovery timeline requirement.

**Campus Response**

We concur. The ITDR plan will identify the specific equipment needed to meet the business recovery timeline requirements and a strategy for acquiring key equipment in the event of a disaster.

Timeline: March 23, 2011

**BACKUP PROCEDURES**

Backup tapes for the library system were rotated off-site to the personal residence of an employee.

SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

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.

EO 1014, *California State University Business Continuity Plan*, dated October 8, 2007, states that the campus must develop plans to protect all critical data assets to ensure minimum data loss and continued business functionality in the event of a disaster.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplant by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The IT consultant, library systems, stated that the campus wanted an affordable option for safeguarding the backup tapes. He was not aware that the CSU did not approve of storing tapes at personal residences.
Failure to appropriately protect sensitive data and ensure that the potential for data loss is minimized could expose the campus and the CSU to legal and financial damages.

**Recommendation 4**

We recommend that the campus discontinue the practice of storing backup tapes for the library at an employee’s personal residence and devise and implement a more secure method for remote storage.

**Campus Response**

We concur. Library backup tapes are now stored off-site and integrated into the campus tape rotation schedule. The campus has contracted with Iron Mountain to provide secure remote storage of backup tapes. Library tapes were moved off-site on August 24, 2010.

Timeline: October 29, 2010

**END-USER COORDINATION AND RESTORATION PROCEDURES**

IT recovery expectations had not been clearly communicated to the individual business units.

Specifically, we noted that I&ITS had not coordinated with the individual business units to convey that:

- Data processing outages may last for an extended period of time, and manual desk procedures may need to be followed until the systems could be restored.

- Some data could be completely lost, and manual recovery procedures should include a step to verify the state of the recovered data and determine which data must be re-created from alternative sources.

SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

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.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, states that the campus shall have each critical business unit perform a business impact assessment to determine the financial and non-financial losses associated with, among other items, a loss of data processing capabilities.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.
The I&ITS director stated that the lack of coordination between the business units and I&ITS occurred because business continuity planning had not been previously conducted at the campus. He also stated that data recovery expectations were being included in the current planning process. The vice president/chief financial officer, administrative affairs, stated that manual desk procedures existed for most departments but that they did not include steps for reconciling the status of recovered data or for re-creating data that may have been lost during the system failure.

Failure to understand the needs of the critical business units and not communicating potential outage impacts to end users increases the likelihood that the campus will not be adequately prepared or be able to effectively respond to an extended outage of data processing services.

**Recommendation 5**

We recommend that the campus:

a. Communicate the possible length of data processing outage and lost data to the individual business units.

b. Update the end-user manual processing desk procedure to include provisions for reconciling the status of the recovered system and re-creating lost data.

**Campus Response**

We concur.

a. The possible length of the data processing outage will be documented in the ITDR plan and reviewed with the individual business units.

b. End-user recovery procedures will be developed to minimize the impact of a disruption in critical IT services.

Timeline: March 23, 2011

**DISASTER RECOVERY PLANNING**

**WRITTEN DISASTER RECOVERY PLAN**

There was no current written plan for the overall recovery of IT services.

We noted that recovery strategies had been completed for each of the IT areas, but there was no overarching documented plan that outlined the specific steps that should be followed in a local disaster.
We also noted that existing disaster recovery plan documentation:

- Did not cross-reference other plans that contain steps that are essential to a recovery process, such as the campus’ emergency procedures, escalation and notification procedures, and use of the emergency command center and public communications.

- Did not provide a step-by-step set of instructions detailing what, when, where, and how action should be taken immediately preceding, during, and following an emergency event, or who should be performing each action.

- Was not sufficient to allow a competent individual who is not directly familiar with the campus’ system to restore the systems and hardware without undue delay, research, and/or guesswork.

SAM §5355.1 states that a disaster recovery plan should be designed such that the requirement for decision-making during and after an event is minimized and individuals are provided direction in as clear and concise a manner as possible. Also, disaster recovery plans must be viable, fully documented, and tested.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, states that the campus must keep all business continuity-related plans current, must test all plans for viability, and must reference all materials necessary to recover from a disaster.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The I&ITS director stated that the campus previously had a documented recovery plan for data processing services but that it was being redesigned as part of the campus business continuity planning process that has not yet been completed. He further stated that the I&ITS portion of the business continuity planning process had been completed.

The absence of a current, tested, and easily executable disaster recovery plan can result in unnecessary financial and non-financial losses in the event of a disaster and can create recovery delays that are outside of management expectations.

**Recommendation 6**

We recommend that the campus document a plan for the overall recovery of IT services.

**Campus Response**

We concur. An overall plan for the recovery of IT services will be documented in the campus ITDR plan.

Timeline: March 23, 2011
DISASTER RECOVERY PLAN TESTING

The campus had not designed a comprehensive plan to test the recovery plan strategies.

SAM §5355.1 states that a disaster recovery plan should be designed such that the requirement for decision-making during and after an event is minimized and individuals are provided direction in as clear and concise a manner as possible. In addition, disaster recovery plans must be viable, fully documented, and tested.

EO 1014, California State University Business Continuity Program, dated October 8, 2007, states that the campus must keep all business continuity-related plans current, must test all plans for viability, and must reference all materials necessary to recover from a disaster.

ICSUAM §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The I&ITS director stated that some aspects of the recovery strategy had been informally tested through periodic interruptions of service, but that formal detailed tests of the overall recovery plan had not been routinely performed.

The absence of a current, tested, and easily executable disaster recovery plan can result in unnecessary financial and non-financial losses in the event of a disaster and can create recovery delays that are outside of management expectations.

**Recommendation 7**

We recommend that the campus design a comprehensive plan to test the recovery plan strategies.

**Campus Response**

We concur. The ITDR plan will include a comprehensive plan to recover critical IT services.

Timeline: March 23, 2011
## 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</td>
</tr>
<tr>
<td>Edwin Barnes</td>
<td>Vice President/Chief Financial Officer, Administrative Affairs</td>
</tr>
<tr>
<td>Stephanie Doda</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Lisa Dye</td>
<td>Business Continuity Coordinator</td>
</tr>
<tr>
<td>Timothy He</td>
<td>Information Technology Consultant, Library Systems</td>
</tr>
<tr>
<td>Joe Matsumoto</td>
<td>Director, Instructional &amp; Information Technology Systems (I&amp;ITS)</td>
</tr>
<tr>
<td>Debbi McFall</td>
<td>Emergency Services Coordinator</td>
</tr>
<tr>
<td>Kevin Morningstar</td>
<td>Executive Director, Student Affairs Technology Service</td>
</tr>
<tr>
<td>Susan Reese</td>
<td>Manager, I&amp;ITS Projects &amp; Services</td>
</tr>
<tr>
<td>Glendy Yeh</td>
<td>Executive Director, Administrative Affairs Information Systems</td>
</tr>
</tbody>
</table>
October 11, 2010

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 to Recommendations of IT Disaster Recovery 10-33

Enclosed is California State Polytechnic’s campus response to the IT Disaster Recovery Audit 10-33. 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,

Edwin A. Barnes, III, Vice President  
Administrative Affairs

Cc: J. Michael Ortiz, President  
Stephanie Doda, Chief Information Officer, Instructional & Information Technology  
Darwin Labordo, Associate Vice President, Finance & Administrative Services  
Sharon Reiter, Associate Vice President, Human Resource Services  
Joice Xiong, University Auditor

Enclosure
BUSINESS IMPACT ASSESSMENT

Recommendation 1

We recommend that the campus complete the business impact assessment and evaluate the ITDR plan against the business requirements for the recovery of data processing services.

Campus Response

We concur. The campus is working toward the completion of the business impact assessment portion of the business continuity plan. The findings of the business impact assessment will be used in the assignment of recovery priorities among business processes and the applications and infrastructures that support them. The findings of the business impact assessment will also be used to validate the recovery time objectives of the existing ITDR plans.

- Complete Business Impact Assessments by December 17, 2010
- Use findings of the Business Impact Assessments to validate the recovery time objectives of the ITDR plan by March 23, 2011

Timeline: March 23, 2011

ALTERNATE PROCESSING

ALTERNATE PROCESSING FACILITY

Recommendation 2

We recommend that the campus:

a. Formalize and document the plan to relocate to another data processing facility on campus and share this information with the campus community.

b. Determine the equipment that would need to be located to the alternate facility and validate that the facility can accommodate the additional equipment.
Campus Response

We concur.

a. The ITDR plan will address the relocation and resumption of critical IT services provided by the primary data processing facility to an alternate location on and off-campus.

b. The plan for the alternate data processing facility will address all equipment needs and consider strategies to reduce the disruption of critical IT services.

Timeline: March 23, 2011

ALTERNATE PROCESSING EQUIPMENT

Recommendation 3

We recommend that the campus document the specific equipment that it would need to replace immediately after a disaster, as well as a strategy for acquiring such equipment in time to meet the business recovery timeline requirement.

Campus Response

We concur. The ITDR plan will identify the specific equipment needed to meet the business recovery timeline requirements and a strategy for acquiring key equipment in the event of a disaster.

Timeline: March 23, 2011

BACKUP PROCEDURES

Recommendation 4

We recommend that the campus discontinue the practice of storing backup tapes for the library at an employee’s personal residence and devise and implement a more secure method for remote storage.

Campus Response

We concur. Library backup tapes are now stored off-site and integrated into the campus tape rotation schedule. The campus has contracted with Iron Mountain to provide secure remote storage of backup tapes. Library tapes were moved off-site on August 24, 2010.

Timeline: October 29, 2010
END-USER COORDINATION AND RESTORATION PROCEDURES

**Recommendation 5**

We recommend that the campus:

a. Communicate the possible length of data processing outage and lost data to the individual business units.

b. Update the end-user manual processing desk procedure to include provisions for reconciling the status of the recovered system and re-creating lost data.

**Campus Response**

We concur.

a. The possible length of the data processing outage will be documented in the ITDR plan and reviewed with the individual business units.

b. End user recovery procedures will be developed to minimize the impact of a disruption in critical IT services.

Timeline: March 23, 2011

DISASTER RECOVERY PLANNING

**WRITTEN DISASTER RECOVERY PLAN**

**Recommendation 6**

We recommend that the campus document a plan for the overall recovery of IT services.

**Campus Response**

We concur. An overall plan for the recovery of IT services will be documented in the Campus ITDR plan.

Timeline: March 23, 2011
DISASTER RECOVERY PLAN TESTING

Recommendation 7

We recommend that the campus design a comprehensive plan to test the recovery plan strategies.

Campus Response

We concur. The ITDR plan will include a comprehensive plan to recover critical IT services.

Timeline: March 23, 2011
November 22, 2010

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Charles B. Reed
       Chancellor

SUBJECT: Draft Final Report 10-33 on IT Disaster Recovery, California State Polytechnic University, Pomona

In response to your memorandum of November 22, 2010, I accept the response as submitted with the draft final report on IT Disaster Recovery, California State Polytechnic University, Pomona.

CBR/amd