## CONTENTS

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

Introduction ................................................................................................................................................... 3
  Background .............................................................................................................................................. 3
  Purpose ..................................................................................................................................................... 4
  Scope and Methodology .......................................................................................................................... 5

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Data Classification ....................................................................................................................................... 6

Asset Management ........................................................................................................................................ 7

Human Resources ........................................................................................................................................ 7
  Information Security Awareness .............................................................................................................. 7
  Background Checks ................................................................................................................................. 9

Network Security ........................................................................................................................................ 10

Access Controls ........................................................................................................................................ 10
  User Access Review .............................................................................................................................. 10
  Server Room Security ............................................................................................................................ 11
  Protection of Paper Documents ............................................................................................................ 12

Encryption ................................................................................................................................................... 13

External Parties ........................................................................................................................................... 14
CONTENTS

APPENDICES

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

ABBREVIATIONS

CSU           California State University
HR            Human Resources
ICSUAM        Integrated California State University Administrative Manual
IDS           Intrusion Detection System
ISO           Information Security Officer
SFSU          San Francisco State University
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2012, the Board of Trustees, at its January 2013 meeting, directed that Sensitive Data Security and Protection be reviewed. The Office of the University Auditor had previously reviewed sensitive data at six campuses in 2011.

We visited the San Francisco State University campus from July 29, 2013, through August 30, 2013, and audited the procedures in effect at that time.

In our opinion, except for the effect of the weaknesses described below, the fiscal, operational, and administrative controls for sensitive data as of August 30, 2013, taken as a whole, were not sufficient to meet the objectives stated above and in the “Purpose” section of this report. Areas of major concern include: data classification, asset management, human resources, network security, access controls, encryption, and external parties.

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 sensitive data, but was designed to assess management controls, increase awareness of the topic, and assess regulatory compliance for significant sensitive data 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.

DATA CLASSIFICATION [6]

The campus did not perform periodic inventory and controls assessments of all protected data maintained in paper files.

ASSET MANAGEMENT [7]

Electronic data records were not consistently disposed of at the end of the required retention period.

HUMAN RESOURCES [7]

The campus did not require all computer users to complete information security awareness training and did not always distribute to all employees regular updates to policies, standards, procedures, and guidelines related to information security. Further, the campus did not retain evidence that background checks had been performed for all individuals hired into sensitive positions.
NETWORK SECURITY [10]

The campus did not have a network intrusion detection system in place to monitor and respond to potential security threats.

ACCESS CONTROLS [10]

The campus did not perform periodic, documented reviews of user access privileges for the human resources system. Also, servers containing sensitive data were maintained in facilities that did not have sufficient physical and environmental controls. Additionally, physical security of paper documents containing sensitive information was inadequate. For example, some sensitive paper documents that contained level 1 and level 2 data were maintained in file cabinets that were not locked after business hours.

ENCRYPTION [13]

The campus did not encrypt level 1 data stored on systems, file servers, and local workstations.

EXTERNAL PARTIES [14]

The campus library did not have an agreement in place with a third-party service provider that had access to sensitive information.
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 sensitive data. 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.

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.

According to ICSUAM §8000.0, 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.
- Compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection.

The policy further states that auxiliary organizations, external businesses, and organizations that use campus information assets must also follow the CSU Information Security Policy.

State Administrative Manual §5300 defines information security as the protection of information and information systems and equipment from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code §11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection in the California Office of Information Security.

At the CSU campuses, the information security officer has overall responsibility for the security and protection of sensitive data, which extends to all campus departments, colleges, and auxiliary organizations.
PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of sensitive data; to determine the adequacy of controls over the related processes; and to 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, oversight committees, executive-level reporting, and documented policies and procedures.

- A management framework is established to initiate and control the implementation of information security within the organization, and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.

- All assets are accounted for and have a nominated owner/custodian who is responsible for achieving and maintaining appropriate protection of organizational assets, and information is appropriately classified to indicate the expected degree of protection.

- Security responsibilities are addressed with employees prior to the start of employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work.

- Responsibilities and procedures for the management of information processing and service delivery are defined, and technical security controls are integrated within systems and networks.

- Access rights to systems, applications, and business processes surrounding sensitive data are controlled by means of user identification and authentication, based on business and security requirements.

- Formal event reporting and escalation procedures are in place for information security events and weaknesses, and communication is consistent and effective, allowing for timely corrective action.

- The information systems’ design, configuration, operation, use, and management are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.

- Contractual language addressing a third party’s responsibility for protecting sensitive data is appropriate.
SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 22 and 23, 2013, meeting of the Committee on Audit, stated that sensitive data security and protection would include review and compliance with Trustee policy, federal and state directives, and campus policies and procedures; procedures for handling confidential information; communication and employee training; encryption; tracking and monitoring of access to sensitive data; and retention practices for key records. If the sensitive data is maintained by a third party, we would review the involvement of campus information security personnel in the decision process; documentation of campus expectations for handling and securing the data; contract language covering security expectations; and monitoring of third-party performance.

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 whether fiscal, 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 security and protection of sensitive data. Specifically, we reviewed and tested:

- Information security policies and procedures.
- Information security organizational structure and management framework.
- Information asset management accountability and classification.
- Human resources security responsibilities.
- Administrative and technical security procedures.
- Access and configuration controls over networks, systems, applications, business processes, and data.
- Incident response, escalation, and reporting procedures.
- Compliance with relevant statutory, regulatory, and contractual security requirements.
- Third-party contractual language regarding handling of sensitive data.

Our testing and methodology was designed to provide a managerial level review of key security practices over sensitive data. Our review did not examine all categories of sensitive data; selected emerging technologies were excluded from the scope of the review. Our testing approach was designed to provide a view of the security used to protect only key computing and business processes.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

DATA CLASSIFICATION

The campus did not perform periodic inventory and controls assessments of all protected data maintained in paper files.

Integrated California State University Administrative Manual (ICSUAM) §8020, Information Security Risk Management, dated April 19, 2010, states that campuses must develop risk management processes that identify, assess, and monitor risks to information assets containing level 1 and level 2 data as defined in the California State University (CSU) Data Classification Standard. Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts. Risk assessments are part of an ongoing risk management process. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls. Campuses must document the scope and frequency of the assessment, risk assessment methodology, result of the risk assessment, and mitigation strategies designed to address identified risks.

ICSUAM §8065, Information Asset Management, dated April 19, 2010, states that campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

The information security officer (ISO) stated that the campus previously performed surveys of level 1 and level 2 data through questionnaires, but this process was manual and meant the data was only as current as accurately reported by the department. She further stated that the campus was awaiting the systemwide licensing of the risk assessment and sensitive data inventory software that was being piloted by the chancellor’s office; until then, the campus would perform periodic risk assessments of the information technology environment and would maintain a spreadsheet of known level 1 and level 2 systems.

Inadequate accountability over information assets, especially those containing critical or personal confidential information, increases the risk of loss and inappropriate use of campus resources and exposure to information security breaches.

Recommendation 1

We recommend that the campus perform periodic inventory and controls assessments of all protected data maintained in paper files.

Campus Response

A survey questionnaire is planned for release in February 2014, and annually thereafter, on the current storage location and state of security level 1 and level 2 data stored in paper files.
Expected completion date: February 2014

**ASSET MANAGEMENT**

Electronic data records were not consistently disposed of at the end of the required retention period.

Executive Order 1031, *Systemwide Records/Information Retention and Disposition Schedules Implementation*, dated February 27, 2008, states that each campus must ensure appropriate and timely disposal of records/information in accordance with retention and disposition schedule time frames. The campus is responsible for instituting a process for reviewing its records/information as listed on the schedules to determine if they should be destroyed or maintained. At a minimum, this review should be conducted once a year. Additionally, each campus must establish procedures regarding the modification of retention and disposition schedules, as needed, to incorporate records unique to each campus. These schedules must be published by the campus and copies are to be provided to the Office of the Chancellor, upon request.

The ISO stated that some systems in use did not have the ability to parse out specific line items for removal, and as a result, electronic records were maintained indefinitely.

Retention of records beyond their expiration date could make them subject to public records requests and could lead to unnecessary expenditure for their storage and maintenance.

**Recommendation 2**

We recommend that the campus consistently dispose of all electronic data records at the end of the required retention period.

**Campus Response**

The campus has existing policy on these topics, and a reminder will be sent to the campus by January 2014.

Expected completion date: January 2014

**HUMAN RESOURCES**

**INFORMATION SECURITY AWARENESS**

Campus information security awareness required improvement.
Specifically, we found that the campus:

- Did not require all computer users to complete information security awareness training.
- Did not always distribute to all employees regular updates to policies, standards, procedures, and guidelines related to information security.

ICSUAM §8035.100, *Information Security Awareness and Training*, dated April 19, 2010, states that each campus must implement a program for providing appropriate information security awareness and training to employees appropriate to their access to campus information assets. The campus information security awareness program must promote campus strategies for protecting information assets containing protected data. All employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training must be provided to individuals whose job functions require specialized skill or knowledge in information security.

ICSUAM §8035.200, dated April 19, 2010, states that the security awareness program must provide an overview of campus information security policies and help individuals recognize and appropriately respond to threats to campus information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. The program must promote awareness of CSU and campus information security policies, standards, procedures, and guidelines; potential threats against campus protected data and information assets; appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets; and CSU and campus notification procedures in the event protected data is compromised. After receiving initial security awareness training, employees must receive regular updates in policies, standards, procedures, and guidelines.

The ISO stated that the campus planned to implement the new security awareness training being licensed to all campuses systemwide via the chancellor’s office, rather than investing additional resources into the current training program to track and monitor the completion of training for all computer users. She further stated that the new program was dependent on CMS and HRMS modules of PeopleSoft. In addition, she stated that the campus had an information technology governance model whereby one committee was regularly briefed and sent updates on information security matters, and that these committee members were responsible for informing their departments about these updates. Also, the ISO stated that she partners with enrollment management to send out semiannual notifications for security reminders once per semester.

Lack of information security awareness training and updates for employees with access to computer resources increases the risk of mismanagement of protected data, increases campus exposure to security breaches, and could compromise compliance with statutory requirements.
**Recommendation 3**

We recommend that the campus:

a. Require all computer users to complete information security awareness training.

b. Distribute to all employees regular updates to policies, standards, procedures, and guidelines related to information security.

**Campus Response**

The campus plans to deploy the Security Awareness Training module from LawRoom and distribute a reminder email of policies, standards, procedures, and guidelines related to information security to all employees.

Expected completion date: February 2014

**BACKGROUND CHECKS**

The campus did not retain evidence that background checks had been performed for all individuals hired into sensitive positions.

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 1 information assets as defined in the CSU Data Classification Standard.

Coded memorandum Human Resources (HR) 2005-10, *Background Checks*, dated March 1, 2005, states that it is the campus’ responsibility to maintain confidentiality of background check information.

The director of faculty and staff employment services/HR management systems stated that the hiring departments were responsible for retaining evidence of completed background checks for individuals hired into sensitive positions.

A lack of background checks for personnel hired into sensitive positions increases the risk of potential misuse or inappropriate disclosure of sensitive data.

**Recommendation 4**

We recommend that the campus maintain evidence that background checks have been performed for all employees hired into sensitive positions.
Campus Response

The campus will maintain evidence of background checks.

Expected completion date: February 2014

NETWORK SECURITY

The campus did not have a network intrusion detection system (IDS) in place to monitor and respond to potential security threats.

ICSUAM §8045.100, Information Technology Security, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

The ISO stated that the campus did not have a network IDS in place due to resource constraints and that advanced technologies had been recommended but were deemed too costly. She further stated that discussions have been under way with the chancellor’s office for more than a year on how to build these capabilities into the existing systemwide networking budget and backbone consistent with systemwide plans for future central management and aggregated incident tracking.

The lack of a network IDS for the monitoring of and response to potential security threats increases campus exposure to information security breaches.

Recommendation 5

We recommend that the campus implement a network IDS to monitor and respond to potential security threats.

Campus Response

Advanced application firewalls were installed on October 25, 2013, for high-risk areas with level 1 and level 2 data to help monitor and prevent advanced security threats.

ACCESS CONTROLS

USER ACCESS REVIEW

The campus did not perform periodic, documented reviews of user access privileges for the HR system.
ICSUAM §8060, Access Control, dated April 19, 2010, states that 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.

The director of faculty and staff employment services/HR management systems stated that daily queries were run to remove inactive users from the system; however, a process is being developed to review user access privileges on a periodic basis.

Inadequate reviews of user access privileges increase the risk of unauthorized or inappropriate exposure to sensitive data and can adversely affect campus compliance with existing regulations regarding protection of such data.

Recommendation 6

We recommend that the campus perform and document periodic reviews of user access privileges for the HR system.

Campus Response

The campus will perform and document periodic reviews of user access privileges for the HR systems.

Expected completion date: February 2014

SERVER ROOM SECURITY

Servers containing sensitive data were maintained in facilities that did not have sufficient physical and environmental controls.

Specifically, we found that:

- One department maintained a server with sensitive data underneath a desk that was located in the general office area.

- The server room for one department did not contain a security alarm system, temperature and humidity monitoring device, smoke detection system, fire extinguisher, or automatic fire suppression system.

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

The ISO stated that physical security of college and departmental server rooms was inadequate because some decentralized areas were not consistently following campus policy and standards.

Lack of adequate physical security and environmental controls over computing equipment increases the risk of information security breaches, theft, and accidental damage to the systems.

**Recommendation 7**

We recommend that the campus maintains servers containing sensitive data in facilities that have sufficient physical and environmental controls.

**Campus Response**

We are working with appropriate departments to transition the servers with sensitive data into the DoIT data center.

Expected completion date: May 2014

**PROTECTION OF PAPER DOCUMENTS**

Physical security of paper documents containing sensitive information was inadequate.

Specifically, we found that:

- Some documents that contained level 1 and level 2 data were maintained in file cabinets that were not locked after business hours.
- Custodial workers had access to rooms that contained unsecured sensitive paper documents.

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.

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. 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.

The ISO stated that physical security of sensitive paper documents was inadequate because some decentralized business units were not consistently following campus policy and standards.

Inadequate physical security over sensitive paper documents increases the risk of information security breaches and unauthorized access.

**Recommendation 8**

We recommend that the campus:

a. Secure all sensitive paper documents in locked filing cabinets.

b. Restrict access to sensitive paper documents to only those with a need to know, or implement other mitigating controls to protect the data.

**Campus Response**

The campus has had policies in place to address the security of sensitive documents, and a reminder on policy will be sent to all faculty and staff by January 2014.

Expected completion date: January 2014

**ENCRYPTION**

The campus did not encrypt level 1 data stored on systems, file servers, and local workstations.

San Francisco State University (SFSU) *Safeguarding Information Policy* states that in the exceptional case when there is a requirement to store confidential data on a desktop, laptop, or other device, special security measures such as encryption must be employed.

SFSU *Server Security Policy* states that sensitive or protected data must be encrypted when at rest (stored) on the computer.

ICSUAM §8045, *Information Technology Security*, dated April 19, 2010, states that each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

ICSUAM §8065, *Information Asset Management*, dated April 19, 2010, states that campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU
Data Classification Standard and that these assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

The ISO stated that protected data maintained on systems, file servers, and local workstations were not always stored in an encrypted format despite policy and technical standards requiring encryption. She also stated that for new system purchases, the campus had specifications to ensure the systems purchased could support encryption. Additionally, the ISO stated that as the campus was migrating to PeopleSoft campus solutions, it was re-examining the means and uses of downloaded data, particularly sensitive data from CMS, to determine whether there was a real need to work with and store this data outside of PeopleSoft. She further stated that the campus was looking at circumstances where level 1 and level 2 data was created by business units and whether there was a need to create local stores of sensitive information.

Lack of encryption for protected data increases the risk of loss or inappropriate use of such data and increases the risk of information security breaches, which could require the campus to notify all affected parties, adversely affecting the campus’ reputation.

**Recommendation 9**

We recommend that the campus encrypt level 1 data stored on systems, file servers, and local workstations.

**Campus Response**

The campus has had a policy for encrypting level 1 data since 2009: http://tech.sfsu.edu/policy/confidential-data. Beginning in March 2014, department information technology will have to document a rationale or alternative risk mitigation in their change requests, deployment tickets, or any implementation that does not include encryption in some form.

Expected completion date: April 2014

**EXTERNAL PARTIES**

The campus library did not have an agreement in place with a third-party service provider that had access to sensitive information.

We found that:

- The campus did not have a contractual agreement including terms for data confidentiality, information security, and system backups with Shiftboard, a hosted scheduling application used by the library that allowed employees to enter patrons’ contact information, including personal phone numbers and home addresses.
The procurement department and the ISO were not involved in the selection and contract process for Shiftboard.

ICSUAM §8040, *Managing Third Parties*, states that third parties who access CSU information assets must be required to adhere to appropriate CSU and campus information security policies and standards. As appropriate, a risk assessment must be conducted to determine the specific implications and control requirements for the service provided. Additionally, third-party service providers must not be granted access to campus level 1 or level 2 information assets as defined in the CSU Data Classification Standard until the access has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.

The university librarian stated that a contractual agreement with Shiftboard was not in place because she was unaware that the services required a contract.

The absence of a signed agreement detailing information security and data confidentiality responsibilities with external parties who have access to sensitive information subjects the campus to potential liability, increases the likelihood of misunderstandings for services provided, and could compromise compliance with statutory information security requirements.

**Recommendation 10**

We recommend that the campus:

a. Sign an agreement with the service provider that includes appropriate provisions for data confidentiality, information security, and system backup responsibilities.

b. Involve the procurement department and the ISO in the contract process with third-party service providers.

**Campus Response**

The campus has been working with a draft procurement template from the chancellor’s office to address third-party security terms, but it has yet to be centrally finalized. A resource evaluation for the information security office to support review of all contracts involving third parties with procurement and a campus operational policy directing staff of the new guidelines will be completed.

Expected completion date: May 2014
# APPENDIX A:
# PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leslie E. Wong</td>
<td>President</td>
</tr>
<tr>
<td>Eva Allen</td>
<td>Associate, Academic and Institutional Studies</td>
</tr>
<tr>
<td>Michelle Anolin</td>
<td>Information Technology Consultant, Division of Information Technology</td>
</tr>
<tr>
<td>Zoila Baltodano</td>
<td>Business Office Manager, Cesar Chavez Student Center</td>
</tr>
<tr>
<td>Brian Beatty</td>
<td>Associate Vice President, Academic Affairs Operations</td>
</tr>
<tr>
<td>Maggie Beers</td>
<td>Director, Academic Technology</td>
</tr>
<tr>
<td>Nicole Bohn</td>
<td>Director, Disability Programs and Research Center</td>
</tr>
<tr>
<td>Avi Chandiramani</td>
<td>Information Technology Consultant, Disability Programs and Research Center</td>
</tr>
<tr>
<td>Ronald Cortez</td>
<td>Vice President of Administration and Finance/Chief Financial Officer</td>
</tr>
<tr>
<td>Guy Dalpe</td>
<td>Managing Director, Cesar Chavez Student Center</td>
</tr>
<tr>
<td>Elizabeth Detrich</td>
<td>Administrative Analyst/Specialist, Library</td>
</tr>
<tr>
<td>Darryl Dieter</td>
<td>Director, Institutional Research</td>
</tr>
<tr>
<td>Tuan Do</td>
<td>Operating System Analyst, Enrollment Management</td>
</tr>
<tr>
<td>Derethia Duval</td>
<td>Director, Counseling and Psychological Services</td>
</tr>
<tr>
<td>Teresa Dziadu</td>
<td>Associate, Academic and Institutional Studies</td>
</tr>
<tr>
<td>Gerard Enriquez</td>
<td>Information Technology Consultant, Development Office</td>
</tr>
<tr>
<td>Charlotte Ferretti</td>
<td>Professor, College of Health and Social Sciences</td>
</tr>
<tr>
<td>Lucas Ford</td>
<td>Analyst/Programmer, College of Health and Social Sciences</td>
</tr>
<tr>
<td>Joellen Fung</td>
<td>Director, Identity Management and Portal</td>
</tr>
<tr>
<td>Longin Gogu</td>
<td>Director, Enrollment Management Technology</td>
</tr>
<tr>
<td>Mark Goodrich</td>
<td>Executive Director, University Property Management</td>
</tr>
<tr>
<td>Mig Hofmann</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Barbara Hubler</td>
<td>Director, Financial Aid</td>
</tr>
<tr>
<td>Patricia Irvine</td>
<td>Associate Dean, Graduate College of Education</td>
</tr>
<tr>
<td>Craig Johnson</td>
<td>Information Technology Consultant, Academic Planning and Development</td>
</tr>
<tr>
<td>Carlos Romero-Julio</td>
<td>Information Technology Consultant, Graduate College of Education</td>
</tr>
<tr>
<td>Betsy Kean</td>
<td>Director, College of Education</td>
</tr>
<tr>
<td>Hao Khuu</td>
<td>Information Technology Consultant, Development Office</td>
</tr>
<tr>
<td>Phoebe Kwan</td>
<td>Associate Vice President and Chief Technology Officer</td>
</tr>
<tr>
<td>Thoreau Lovell</td>
<td>Associate, Academic and Institutional Studies</td>
</tr>
<tr>
<td>Franz Lozano</td>
<td>Associate Vice President, University Budget and Operations</td>
</tr>
<tr>
<td>Michael Martin</td>
<td>Interim Associate Vice President, Human Resources, Safety and Risk</td>
</tr>
<tr>
<td>Deborah Masters</td>
<td>University Librarian</td>
</tr>
<tr>
<td>Martin Masters</td>
<td>Information Technology Consultant, Division of Information Technology</td>
</tr>
<tr>
<td>Charles Meyer</td>
<td>Director, Facilities and Service Enterprises</td>
</tr>
<tr>
<td>Stephen Henry McCoy</td>
<td>Director, Faculty and Staff Employment Services/Human Resources</td>
</tr>
<tr>
<td>Renee Monte</td>
<td>University Registrar/Privacy Officer</td>
</tr>
<tr>
<td>Delma Munoz</td>
<td>Manager, Campus Support Services</td>
</tr>
<tr>
<td>Teresa Ono</td>
<td>Director of Special Events, University Advancement</td>
</tr>
<tr>
<td>Stanley Pearse</td>
<td>Administrative Analyst/Specialist, Fiscal Affairs</td>
</tr>
</tbody>
</table>
APPENDIX A: PERSONNEL CONTACTED

Vernon Piccinotti  Technical Services/Information Technology Manager, Cesar Chavez Student Center
Kenneth Piper  Operating System Analyst, Enrollment Management
Andrew Roderick  Information Technology Consultant, Academic Technology
David Rourke  Manager, Planning and Personnel
Karrie Drew Schmid  Administrative Analyst/Specialist, University Property Management
Wendy Schweitzer  Associate, Academic and Institutional Studies
Alastair Smith  Director, Student Health
Stephen Smith  Director, Procurement
Andy Stockton  Information Technology Consultant, University Property Management
Venesia Thompson  Chief of Operations, University Advancement
Kasra Varzaghani  Associate, Academic and Institutional Studies
Patrick Wachira  Security Administrator, Human Resources
Georgianna Wong  Administrative Analyst/Specialist, Library
Ewa Zachoszcz  Administrative Analyst/Specialist, Graduate College of Education
December 16, 2013

Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, California 90802-4275

Dear Larry:

We have reviewed Audit Report #13-32, Sensitive Data Security and Protection, from your office and are providing our responses to the recommendations electronically as requested.

Questions regarding the responses should be directed to Ron S. Cortez, Vice President and CFO, Administration and Finance at (415) 338-2521 or to Maureen Pasag, Director of Internal Audit at (415) 405-4343.

Sincerely,

Dr. Les Wong
President

RC/FL/id

Attachment

cc: Ron S. Cortez, Vice President and CFO, Administration and Finance
Phoebe Kwan, Associate Vice President and Chief Technology Officer, DoIT
Michael Martin, Interim Associate Vice President, Human Resources, Safety & Risk
Mig Hofmann, Information Security Officer, DoIT
S. Henry McCoy, Director, Fac. & Staff Employment Svcs / HR Mgmt. Syst,HRSRM
Franz Lozano, Associate Vice President, Budget Administration & Operations
Maureen Pasag, Director, Internal Audit
SENSITIVE DATA SECURITY AND PROTECTION

SAN FRANCISCO STATE UNIVERSITY

Audit Report 13-32

DATA CLASSIFICATION

Recommendation 1

We recommend that the campus perform periodic inventory and controls assessments of all protected data maintained in paper files.

Campus Response
A survey questionnaire is planned for release in February 2014, and annually thereafter, on the current storage location and state of security level 1 and level 2 data stored in paper files.

Expected completion date: February 2014

ASSET MANAGEMENT

Recommendation 2

We recommend that the campus consistently dispose of all electronic data records at the end of the required retention period.

Campus Response
The campus has existing policy on these topics, and a reminder will be sent to the campus by January 2014.

Expected completion date: January 2014

HUMAN RESOURCES

INFORMATION SECURITY AWARENESS

Recommendation 3

We recommend that the campus:

a. Require all computer users to complete information security awareness training.

b. Distribute to all employees regular updates to policies, standards, procedures, and guidelines related to information security.
Campus Response

The campus plans to deploy the Security Awareness Training module from LawRoom and distribute a reminder email of policies, standards, procedures, and guidelines related to information security to all employees.

Expected completion date: February 2014

BACKGROUND CHECKS

Recommendation 4

We recommend that the campus maintain evidence that background checks have been performed for all employees hired into sensitive positions.

Campus Response

The campus will maintain evidence of background checks.

Expected completion date: February 2014

NETWORK SECURITY

Recommendation 5

We recommend that the campus implement a network IDS to monitor and respond to potential security threats.

Campus Response

Advanced application firewalls were installed on October 25, 2013, for high-risk areas with level 1 and level 2 data to help monitor and prevent advanced security threats.

ACCESS CONTROLS

USER ACCESS REVIEW

Recommendation 6

We recommend that the campus perform and document periodic reviews of user access privileges for the HR system.

Campus Response

The campus will perform and document periodic reviews of user access privileges for the HR systems.
Expected completion date: February 2014

SERVER ROOM SECURITY

Recommendation 7

We recommend that the campus maintain servers containing sensitive data in facilities that have sufficient physical and environmental controls.

Campus Response

We are working with appropriate departments to transition the servers with sensitive data into the DoIT data center.

Expected completion date: May 2014

PROTECTION OF PAPER DOCUMENTS

Recommendation 8

We recommend that the campus:

a. Secure all sensitive paper documents in locked filing cabinets.

b. Restrict access to sensitive paper documents to only those with a need to know, or implement other mitigating controls to protect the data.

Campus Response

The campus has had policies in place to address the security of sensitive documents and a reminder on policy will be sent to all faculty and staff by January 2014.

Expected completion date: January 2014

ENCRYPTION

Recommendation 9

We recommend that the campus encrypt level 1 data stored on systems, file servers, and local workstations.

Campus Response

The campus has had a policy for encrypting level 1 data since 2009: http://tech.sfsu.edu/policy/confidential-data. Beginning in March 2014, department information technology will have to document a rationale or alternative risk mitigation in their change requests or deployment tickets or any implementation that does not include encryption in some form.
Expected completion date: April 2014

EXTERNAL PARTIES

Recommendation 10

We recommend that the campus:

a. Sign an agreement with the service provider that includes appropriate provisions for data confidentiality, information security, and system backup responsibilities.

b. Involve the procurement department and the ISO in the contract process with third-party service providers.

Campus Response

The campus has been working with a draft procurement template from the chancellor’s office to address third-party security terms, but it has yet to be centrally finalized. A resource evaluation for the information security office to support review of all contracts involving third parties with procurement and a campus operational policy directing staff of the new guidelines will be completed.

Expected completion date: May 2014
January 23, 2014

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Timothy P. White
      Chancellor

SUBJECT: Draft Final Report 13-32 on
        *Sensitive Data Security and Protection*,
        San Francisco State University

In response to your memorandum of January 23, 2014, I accept the response as submitted with the draft final report on *Sensitive Data Security and Protection*, San Francisco State University.

TPW/amd