CONTENTS

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

Introduction .......................................................................................................................................................... 2
  Background ....................................................................................................................................................... 2
  Purpose .............................................................................................................................................................. 3
  Scope and Methodology .................................................................................................................................. 4

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance ........................................................................................................................................... 5
APPENDICES

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

ABBREVIATIONS

CSU California State University
ICSUAM Integrated California State University Administrative Manual
ISO Information Security Officer
IT Information Technology
ITS Information Technology Services
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2010, the Board of Trustees, at its January 2011 meeting, directed that Sensitive Data Security and Protection be reviewed. The Office of the University Auditor had previously reviewed some aspects of sensitive data in the 2008 and 2009 audits of Information Security.

We visited the California State University, Los Angeles campus from October 3, 2011, through October 28, 2011, and audited the procedures in effect at that time.

Our study and evaluation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on controls over sensitive data. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report. In our opinion, the operational and administrative controls over sensitive data in effect as of October 28, 2011, 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 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.

SECURITY GOVERNANCE [5]

The campus information security program did not include comprehensive oversight of decentralized departments. Specifically, assessment of sensitive data stored on paper documents was not current, and the annual information technology general controls/best practices gap analyses prepared by each of the departments was not incorporated into the campus information security plan.
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.
INTRODUCTION

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.
The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 25 and 26, 2011, 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 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 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

SECURITY GOVERNANCE

The campus information security program did not include comprehensive oversight of decentralized departments.

For example, we found that:

- The assessment of sensitive data stored on paper documents was not current.

- The annual information technology (IT) general controls/best practices gap analyses prepared by each of the departments was not incorporated into the campus information security plan.

Integrated California State University Administrative Manual (ICSUAM) §8010.00, Establishing an Information Security Program, states in part, that the campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The program should include, among others: a) provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic), b) develop risk management strategies to identify and mitigate threats and vulnerabilities.

ICSUAM §8015, Organizing Information Security, states in part that the information security officer (ISO) (or designee of president) is responsible for the campuswide information security program and may organize the responsibilities as appropriate.

ICSUAM §8020, Information Security Risk Management, 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 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.

The vice president and chief information officer of information technology services stated that other departments had record custodians monitoring the paper documents, and that the ISO is assessing the process only when requested. He also stated that the annual departmental best practices gap analyses were received and reviewed by the campus internal auditor and used as part of the following year’s audit plan.

Inadequate oversight by the information security function could lead to exposure of sensitive data, gaps in internal control, or non-compliance with the information security program.
Recommendation 1

We recommend that the campus ensure that the information security program includes:

a. A current assessment of sensitive data stored on paper and other hard media.

b. An annual review of the departments’ IT general controls/best practices gap analyses and inclusion of the results in the campus information security plan by the ISO.

Campus Response

a. The assessment of sensitive data stored on paper and other hard media was performed in February 2012.

b. The campus revised its procedures in February 2012 requiring each division to submit the information security risk assessment annually to the ISO. The results will then be reviewed and incorporated into the campus risk assessment.
## APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>James M. Rosser</td>
<td>President</td>
</tr>
<tr>
<td>Joseph Aguirre</td>
<td>Executive Director, University-Student Union</td>
</tr>
<tr>
<td>Van Andranigian</td>
<td>Information Technology Coordinator, Administrative Technology</td>
</tr>
<tr>
<td>Kevin Brady</td>
<td>Director, Risk Management and Environmental, Health and Safety</td>
</tr>
<tr>
<td>Lisa Chavez</td>
<td>Vice President for Administration and Chief Financial Officer</td>
</tr>
<tr>
<td>Annie Ekshian</td>
<td>Supervisor, Property Management Office</td>
</tr>
<tr>
<td>Gay Galgano</td>
<td>Director, Payroll Services</td>
</tr>
<tr>
<td>Jose Gomez</td>
<td>Associate Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Tanya Ho</td>
<td>University Internal Auditor</td>
</tr>
<tr>
<td>Robert Hoffmann</td>
<td>Assistant Director, Operations and Access Management, Information Technology Services (ITS)</td>
</tr>
<tr>
<td>Steve Jones</td>
<td>Associate Dean, Undergraduate Studies</td>
</tr>
<tr>
<td>Tammie Leung</td>
<td>Director of Outreach and Recruitment, Office of Admissions and Recruitment</td>
</tr>
<tr>
<td>Vince Lopez</td>
<td>Director, Office of Admissions and Recruitment</td>
</tr>
<tr>
<td>Karen Melick</td>
<td>Director, Administrative Technology</td>
</tr>
<tr>
<td>Sheryl Okuno</td>
<td>Director, Information Technology (IT) Security and Compliance</td>
</tr>
<tr>
<td>Rhoda Posey</td>
<td>Associate Director, Center for Student Financial Aid</td>
</tr>
<tr>
<td>Peter Quan</td>
<td>Vice President and Chief Information Officer, ITS</td>
</tr>
<tr>
<td>Chris Rapp</td>
<td>Director, ITS IT Infrastructure Services</td>
</tr>
<tr>
<td>Salvador Rodriques</td>
<td>Senior Internal Auditor</td>
</tr>
<tr>
<td>Lisa Sanchez</td>
<td>Assistant Vice President, Human Resources Management</td>
</tr>
<tr>
<td>Dan Thomas</td>
<td>Risk Management Analyst, Environmental, Health and Safety Office, Division of Administration and Finance</td>
</tr>
<tr>
<td>Rowena Tran</td>
<td>Assistant Director, University-Student Union</td>
</tr>
<tr>
<td>Susie Varela</td>
<td>Director, Human Resource Management</td>
</tr>
<tr>
<td>Intef Weser</td>
<td>Executive Director, Associated Students, Incorporated</td>
</tr>
<tr>
<td>Joan Woosley</td>
<td>Director of Recruitment</td>
</tr>
</tbody>
</table>
February 22, 2012

Mr. Larry Mandel, University Auditor
Office of the University Auditor
Office of the Chancellor – The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210

Re: University’s Response to Recommendations Contained in Report Number 11-52, Sensitive Data Security and Protection

Dear Mr. Mandel:

Attached are the University’s responses to the recommendations contained in Report Number 11-52, Sensitive Data Security and Protection audit.

Please contact Tanya Ho, University Internal Auditor, at (323) 343-5102, if you wish to discuss the matter contained herein.

Sincerely,

James M. Rosser
President

Attachment

cc: (with attachments)
Lisa Chavez, Vice President for Administration and Chief Financial Officer
Peter Quan, Vice President for ITS and Chief Information Officer
Sheryl Okuno, Director, Information Technology Security and Compliance
Tanya Ho, University Internal Auditor
Jill Carnahan, Administrative Compliance Officer
SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY,
LOS ANGELES

Audit Report 11-52

SECURITY GOVERNANCE

Recommendation 1

We recommend that the campus ensure that the information security program includes:

a. A current assessment of sensitive data stored on paper and other hard media.

b. An annual review of the departments’ IT general controls/best practices gap analyses and inclusion of the results in the campus information security plan by the ISO.

Campus Response

a. The assessment of sensitive data stored on paper and other hard media was performed in February 2012.

b. The campus revised its procedures in February 2012 requiring each division to submit the Information Security Risk Assessment annually to the ISO. The results will then be reviewed and incorporated into the campus risk assessment.
March 26, 2012

MEMORANDUM

TO: Mr. Larry Mandel University Auditor
FROM: Charles B. Reed Chancellor
SUBJECT: Draft Final Report 11-52 on Sensitive Data Security and Protection, California State University, Los Angeles

In response to your memorandum of March 26, 2012, I accept the response as submitted with the draft final report on Sensitive Data Security and Protection, California State University, Los Angeles.

CBR/amd