SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY,
SACRAMENTO

Audit Report 11-54
November 10, 2011

Members, Committee on Audit

Henry Mendoza, Chair
Melinda Guzman, Vice Chair
Margaret Fortune  Steven M. Glazer
William Hauck   Hsing Kung   Linda Lang

Staff

University Auditor: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditor: Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
CONTENTS

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
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, Sacramento campus from August 15, 2011, through September 16, 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 September 16, 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.

APPLICATION SYSTEM ACCESS [5]

Non-disclosure confidentiality agreements for system users with access to sensitive data were not always properly maintained.
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.
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

APPLICATION SYSTEM ACCESS

Non-disclosure confidentiality agreements for system users with access to sensitive data were not always properly maintained.

We reviewed 20 system users with access to level 1 data as defined in the California State University (CSU) Data Classification Standard, and we found that confidentiality agreements could not be located for nine of them.

Integrated California State University Administrative Manual §8030, Personnel Information Security, dated April 19, 2010, states that users who have access to level 1 or level 2 sensitive data as defined in the CSU Data Classification Standard must sign an approved systemwide confidentiality agreement.

The vice president and chief information officer stated that all employees with regular access to level 1 information are required by policy to sign confidentiality agreements, which are sent to human resources to be maintained in employee personnel files. The vice president of human resources stated that the current system for collecting signed confidentiality agreements was a manual process involving paper forms, which increased the risk of misfiled documents and hindered the ability of staff to easily retrieve the forms.

Failure to obtain and maintain signed confidentiality agreements increases the risk that employees will not understand their security obligations, which could lead to inadvertent security breaches and inadequate disciplinary recourse if such breaches do occur.

Recommendation 1

We recommend that the campus ensure that non-disclosure confidentiality agreements for system users with access to sensitive data are properly maintained.

Campus Response

Information resources and technology (IRT) processes non-disclosure confidentiality agreements signed by system users with access to sensitive data. IRT forwards the confidentiality agreements to human resources (HR). By June 30, 2012, HR will review and strengthen the current process for the maintenance of non-disclosure confidentiality agreements, such that the agreements are promptly filed and accessible. Additionally, HR will communicate the process to applicable staff.
### APPENDIX A:

**PERSONNEL CONTACTED**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander Gonzalez</td>
<td>President</td>
</tr>
<tr>
<td>Tejeshwar Chowdhary</td>
<td>Director and Information Technology Coordinator, Student Affairs</td>
</tr>
<tr>
<td>Mike Christensen</td>
<td>Associate Vice President of Risk Management Services</td>
</tr>
<tr>
<td>Leslie Davis</td>
<td>Executive Director, University Union and The Well</td>
</tr>
<tr>
<td>Emiliano Diaz</td>
<td>Director, Admissions and Outreach</td>
</tr>
<tr>
<td>Jill Farrell</td>
<td>Business Office Manager, University Union and The Well</td>
</tr>
<tr>
<td>Dennis Geyer</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Larry Gilbert</td>
<td>Vice President and Chief Information Officer</td>
</tr>
<tr>
<td>Yavette Hayward</td>
<td>Senior Management Auditor</td>
</tr>
<tr>
<td>Ming-Tung “Mike” Lee</td>
<td>Interim Vice President and Chief Financial Officer, Administration and Business Affairs</td>
</tr>
<tr>
<td>Dena Lemus</td>
<td>Admissions Counselor, Admissions and Outreach</td>
</tr>
<tr>
<td>Cindy Martinez</td>
<td>Enrollment Systems Analyst, Records and Campus Community</td>
</tr>
<tr>
<td>Lynn Maynard</td>
<td>Assistant Director of Financial Aid Systems Operations</td>
</tr>
<tr>
<td>Kathi McCoy</td>
<td>Director of Auditing Services</td>
</tr>
<tr>
<td>Ed Mills</td>
<td>Associate Vice President, Enrollment Services</td>
</tr>
<tr>
<td>Mark Montalvo</td>
<td>Director of Finance and Administration, Associated Students</td>
</tr>
<tr>
<td>Jason Musselman</td>
<td>Network Security Analyst</td>
</tr>
<tr>
<td>Helen Norris</td>
<td>Associate Vice President, Administrative Computing Systems</td>
</tr>
<tr>
<td>Kristine Novak</td>
<td>Assistant Registrar</td>
</tr>
<tr>
<td>Andy Schloss</td>
<td>Director of Hardware and Software Support</td>
</tr>
<tr>
<td>Andrew Singletary</td>
<td>Information Technology Manager, University Union and The Well</td>
</tr>
<tr>
<td>Kirt Stout</td>
<td>Director of Risk Management and Business Continuity Planning</td>
</tr>
<tr>
<td>Elizabeth Sublett</td>
<td>Interim Associate Vice President, Human Resource Services</td>
</tr>
<tr>
<td>Gerald Tubo</td>
<td>Information Technology Manager, Associated Students of California State University, Sacramento</td>
</tr>
<tr>
<td>David Wagner</td>
<td>Vice President of Human Resources</td>
</tr>
<tr>
<td>Jeff Williams</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Patricia Worley</td>
<td>Executive Director, Associated Students of California State University, Sacramento</td>
</tr>
<tr>
<td>Craig Yamamoto</td>
<td>Financial Aid Director</td>
</tr>
</tbody>
</table>
December 16, 2011

Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

SUBJECT: Campus Response to Recommendation
Sensitive Data Security and Protection Audit, Report #11-54

Dear Mr. Mandel,

Please find attached California State University, Sacramento's response to the recommendation of the audit. The campus is committed to addressing and resolving the issue identified in the audit report.

If you have any questions or require additional information, please contact Kathi McCoy, Director of Auditing Services, at 916 278-7439.

Sincerely,

Ming-Tung "Mike" Lee, Ph.D.
Vice President & Chief Financial Officer (Interim)

MTL: kd

Attachment

cc: Alexander Gonzalez, President
David Wagner, Vice President of Human Resources
Elizabeth Sublett, Interim Associate Vice President of Human Resources
Christine Lovely, University Counsel
Larry Gilbert, Vice President and Chief Information Officer
Kathi McCoy, Director, Auditing Services
APPLICATION SYSTEM ACCESS

Recommendation 1

We recommend that the campus ensure that non-disclosure confidentiality agreements for system users with access to sensitive data are properly maintained.

Campus Response

Information Resources & Technology (IRT) processes non-disclosure confidentiality agreements signed by system users with access to sensitive data. IRT forwards the confidentiality agreements to Human Resources (HR).

By June 30, 2012, HR will review and strengthen the current process for the maintenance of non-disclosure confidentiality agreements, such that the agreements are promptly filed and accessible. Additionally, HR will communicate the process to applicable staff.
January 3, 2012

MEMORANDUM

TO: Mr. Larry Mandel  
   University Auditor

FROM: Charles B. Reed  
       Chancellor

SUBJECT: Draft Final Report 11-54 on  
         Sensitive Data Security and Protection,  
         California State University, Sacramento

In response to your memorandum of January 3, 2012, I accept the response as submitted with the draft final report on Sensitive Data Security and Protection, California State University, Sacramento.

CBR/amd