SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA POLYTECHNIC STATE UNIVERSITY,
SAN LUIS OBISPO

Audit Report 11-55
February 21, 2012

Members, Committee on Audit

Henry Mendoza, Chair
Melinda Guzman, Vice Chair
Margaret Fortune   Steven M. Glazer
William Hauck   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

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

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

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

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

Application and System Access .................................................................................................................... 6
APPENDICES

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

ABBREVIATIONS

CIO  Chief Information Officer
CSU  California State University
ICSUAM  Integrated California State University Administrative Manual
ISO  Information Security Officer
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 Polytechnic State University, San Luis Obispo campus from November 14, 2011, through December 9, 2011, and audited the procedures in effect at that time.

Our study and evaluation revealed certain conditions that, in our opinion, could result in significant errors and irregularities if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: security governance and system access. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, except for the effect of the weaknesses described above, the operational and administrative controls over sensitive data in effect as of December 9, 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]

Campus governance and executive management oversight did not ensure that information security risks were corrected or mitigated.

APPLICATION AND SYSTEM ACCESS [6]

Access to student grades was not appropriately restricted to authorized personnel, and the annual system access evaluation process did not include a review of access to student grades.
**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.
INTRODUCTION

SCOPE AND METHODOLOGY

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

Campus governance and executive management oversight did not ensure that information security risks were corrected or mitigated.

Specifically, we found that:

- Information security initiatives and actions taken to correct findings from the prior Information Security audit, performed in 2009, were incomplete.

- The risk level of information security initiatives and the length of time the initiatives had remained open was not reported to executive management.

Integrated California State University Administrative Manual (ICSUAM) §8015, Organizing Information Security, states that each campus must develop, implement, and document the organizational structure that supports the campus’ information security program.

ICSUAM §8015, Information Security Risk Management, states that once a risk has been identified, campuses must develop and implement strategies to reduce the risk to acceptable levels, share or shift the risk to another party, or assume the identified risk.

The director of administration and finance department tech services and information security officer (ISO) stated that due to conflicting demands on IT resources, not all security initiatives had been addressed.

Failure to ensure that information security risks are corrected or mitigated increases the likelihood of security compromises and inadequate security over protected data.

Recommendation 1

We recommend that the campus improve governance and executive management oversight to ensure that:

a. Information security initiatives are completed in a timely manner.

b. The risk level of information security initiatives and the length of time the initiatives remain open is reported.

Campus Response

We concur. The campus chief information officer will implement quarterly reporting of security initiatives to executive management. This report will include items identified in our annual and
ongoing risk assessment processes and will reflect assessed risk and due dates selected based on risk. Reports for the first three quarters of 2012 will be issued on March 30, June 29, and August 31.

All initiatives from our 2011 Annual Information Security Report will be included in these quarterly reports and will be completed by August 31, 2012.

APPLICATION AND SYSTEM ACCESS

Access to student grades was not appropriately restricted to authorized personnel, and the annual system access evaluation process did not include a review of access to student grades.

We found that employees from several campus departments, such as university police, university parking, and the library, had access to student grades.

ICSUAM §8060, Access Control, dated April 19, 2010, states that access to campus information assets containing protected data as defined in the California State University Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task.

State Administrative Manual §4841 states that state agencies must provide for the proper use and protection of information assets by establishing appropriate policies and procedures for preserving the integrity and security of automated files and databases.

The director of administration and finance department tech services and ISO stated that certain access may have been improperly assigned as a result of using default roles and initial preset roles created within the system.

Improper assignment of employee access could lead to unauthorized or inappropriate disclosure of sensitive data and could adversely affect campus compliance with statutory regulations regarding protection of such data.

Recommendation 2

We recommend that the campus:

a. Appropriately restrict access to student grades to authorized personnel.
b. Expand the annual system access evaluation to include a review of access to student grades.

Campus Response

We concur. The campus registrar will review all access to student grades to establish basis for authorization by June 29, 2012.
The campus will implement changes to enforce this basis as part of the access-granting process and to review existing grants on an annual basis. We will implement additional permissions as necessary to separate access to grades from access to other student information for which broader access is appropriate. Personnel who are not authorized to access grades will not be given grade permissions. These changes will be implemented by August 31, 2012.
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeffrey D. Armstrong</td>
<td>President</td>
</tr>
<tr>
<td>Donna Amos</td>
<td>Associate Director, Admissions, Recruitment, Financial Aid</td>
</tr>
<tr>
<td>Debbie Arseneau</td>
<td>Associate Registrar, Office of the Registrar</td>
</tr>
<tr>
<td>Marc Benadiba</td>
<td>Assistant Director for Payroll and Payment Management</td>
</tr>
<tr>
<td>Chris Blackburn</td>
<td>Administrative Analyst, Human Resources</td>
</tr>
<tr>
<td>Martin Braggs</td>
<td>Director, Health and Counseling Services</td>
</tr>
<tr>
<td>Ed Bruns</td>
<td>Network Analyst, Network Administration, Information Technology Services (ITS)</td>
</tr>
<tr>
<td>Chris Call</td>
<td>Information Security Coordinator, Administration and Finance</td>
</tr>
<tr>
<td>Anthony Colvard</td>
<td>Information Technology Consultant, Associated Students, Incorporated</td>
</tr>
<tr>
<td>Ken Delmese</td>
<td>Property Clerk II, Fiscal Services, Property</td>
</tr>
<tr>
<td>Don Duke</td>
<td>Operating Systems Analyst, ITS, LAN Server Services</td>
</tr>
<tr>
<td>Julie Dupuy</td>
<td>Administrative Analyst, Academic Records, System Management</td>
</tr>
<tr>
<td>Brad Fely</td>
<td>Administrative Analyst, Office of the Registrar</td>
</tr>
<tr>
<td>Beth Gallagher</td>
<td>Executive Director, Human Resources</td>
</tr>
<tr>
<td>Mark Goble</td>
<td>Information Technology Consultant, Health and Counseling Services</td>
</tr>
<tr>
<td>Joyce Haretani</td>
<td>Associate Director, Human Resources</td>
</tr>
<tr>
<td>Lawrence Kelley</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Lois Kelly</td>
<td>Director of Financial Aid</td>
</tr>
<tr>
<td>Lorlie Leetham</td>
<td>Director of Fiscal Services, Administration and Finance</td>
</tr>
<tr>
<td>Scott Loosley</td>
<td>Associate Director for Operations, Facility Services</td>
</tr>
<tr>
<td>Dee Louie</td>
<td>Accountant II, Fiscal Services, Financial Reporting</td>
</tr>
<tr>
<td>Johanna Madjedi</td>
<td>Associate Vice Provost, ITS</td>
</tr>
<tr>
<td>Jim Maraviglia</td>
<td>Associate Vice Provost, Admissions, Recruitment, and Financial Aid</td>
</tr>
<tr>
<td>David Mason</td>
<td>Network Analyst, Documents and Technical Services</td>
</tr>
<tr>
<td>Ryan Matteson</td>
<td>Security and Architecture, Office of the Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>Theresa May</td>
<td>Interim Director, Information Services Infrastructure, ITS</td>
</tr>
<tr>
<td>Mike Miller</td>
<td>Vice Provost for Information Services, CIO</td>
</tr>
<tr>
<td>Greg Porter</td>
<td>Operating Systems Analyst, Central Systems Administration, ITS</td>
</tr>
<tr>
<td>Rick Ramirez</td>
<td>Associate Vice President for Finance, Administration and Finance</td>
</tr>
<tr>
<td>Gage Sahl</td>
<td>Warehouse Worker, Facility Services, Moving and Surplus</td>
</tr>
<tr>
<td>Katy Schrempp</td>
<td>Administrative Analyst, Admissions, Recruitment, and Financial Aid</td>
</tr>
<tr>
<td>Lisa Shealy</td>
<td>Information Technology Consultant, Central Systems</td>
</tr>
<tr>
<td>Cem Sunata</td>
<td>Registrar</td>
</tr>
<tr>
<td>Terry Vahey</td>
<td>Director, Administration and Finance Department Tech Services and Information Security Officer</td>
</tr>
<tr>
<td>Richard Walls</td>
<td>Interim Director Communication and Computing Services, ITS</td>
</tr>
</tbody>
</table>
16 March 2012

Mr. Larry Mandel
University Auditor
Office of the University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4275

Subject: Campus Responses to Recommendations of Incomplete Draft Audit Report Number 11-55, Sensitive Data Security and Protection, California Polytechnic State University, San Luis Obispo

Dear Larry:

Enclosed are responses to the recommendations in the incomplete draft of the Sensitive Data Security and Protection audit report (Audit Report No. 11-55). The responses are submitted to you for review and for acceptance by the Chancellor. The responses include a corrective action plan and time frame for completion.

Please direct questions to Rick Ramírez, Associate Vice President for Finance, at 805-756-2091 (tramirez@calpoly.edu).

Sincerely,

[Signature]

Lawrence R. Kelley
Vice President for Administration & Finance

cc: J. Armstrong, R. Ramírez, Michael Miller, Ryan Matteson
SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA POLYTECHNIC STATE UNIVERSITY,
SAN LUIS OBISPO

Audit Report 11-55

SECURITY GOVERNANCE

Recommendation 1

We recommend that the campus improve governance and executive management oversight to ensure that:

a. Information security initiatives are completed in a timely manner.

b. The risk level of information security initiatives and the length of time the initiatives remain open is reported.

Campus Response

Concur. The campus CIO will implement quarterly reporting of security initiatives to executive management. This report will include items identified in our annual and ongoing risk assessment processes and will reflect assessed risk and due dates selected based on risk. Reports for the first three quarters of 2012 will be issued on March 30, June 29, and August 31.

All initiatives from our 2011 Annual Information Security Report will be included in these quarterly reports and will be completed by August 31, 2012.

APPLICATION AND SYSTEM ACCESS

Recommendation 2

We recommend that the campus:

a. Appropriately restrict access to student grades to authorized personnel.

b. Expand the annual system access evaluation to include a review of access to student grades.

Campus Response

Concur. The campus registrar will review all access to student grades to establish basis for authorization by June 29, 2012.
The campus will implement changes to enforce this basis as part of the access granting process and to review existing grants on an annual basis. We will implement additional permissions as necessary to separate access to grades from access to other student information for which broader access is appropriate. Personnel who are not authorized to access grades will not be given grade permissions. These changes will be implemented by August 31, 2012.
March 27, 2012

MEMORANDUM

TO:    Mr. Larry Mandel  
       University Auditor

FROM:  Charles B. Reed  
       Chancellor

SUBJECT: Draft Final Report 11-55 on  
Sensitive Data Security and Protection,  
California Polytechnic State University, San Luis Obispo

In response to your memorandum of March 27, 2012, I accept the response as submitted with the draft final report on Sensitive Data Security and Protection, California Polytechnic State University, San Luis Obispo.

CBR/amd