SENSITIVE DATA SECURITY AND PROTECTION
SONOMA STATE UNIVERSITY

Audit Report 11-50
October 21, 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

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
## CONTENTS

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

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

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance ..................................................................................................................................... 6
  Information Security Organization ........................................................................................................... 6
  Information Security Reporting .............................................................................................................. 6

Asset Management ........................................................................................................................................ 8

Network Security .......................................................................................................................................... 9
  Wireless Encryption .................................................................................................................................. 9
  Firewall Configuration ............................................................................................................................ 9
  Network Segmentation ........................................................................................................................... 10

Information Security Awareness Training .................................................................................................. 11

Application System Access ........................................................................................................................ 12
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
IT   Information Technology
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 Sonoma State University campus from April 18, 2011, through May 27, 2011, and audited the procedures in effect at that time.

Our study and evaluation revealed certain conditions that, in our opinion, could result in inappropriate access or disclosure of sensitive data if not corrected. Specifically, the campus had not implemented adequate controls over the following areas: security governance, asset management, network security, information security awareness training, and application system access. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, due to the effect of the weaknesses described above, the operational and administrative controls over sensitive data in effect as of May 27, 2011, taken as a whole, were not sufficient to meet the objectives stated in the “Purpose” section of this report.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all 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 [6]

The campus organizational structure did not provide appropriate oversight for the information security function. In addition, the process for reporting on information security incidents and initiatives needed improvement. Specifically, the campus did not have a procedure to identify and report all security incidents, and security initiatives were not consistently reported to campus executive management.

ASSET MANAGEMENT [8]

Several campus computers were not subject to information security oversight, as computers managed outside of the information technology department were not tracked, secured, and monitored by the information security office.
NETWORK SECURITY [9]

Campus wireless networks were not configured to encrypt network traffic, and firewall filtering of inbound traffic was not set to automatically deny potentially dangerous network traffic. Also, the campus had not placed Internet-accessible web servers on a separate network segment from other internal production servers.

INFORMATION SECURITY AWARENESS TRAINING [11]

Faculty members with access to student records were not required to complete information security awareness training.

APPLICATION SYSTEM ACCESS [12]

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

INFORMATION SECURITY ORGANIZATION

The campus organizational structure did not provide appropriate oversight for the information security function.

We found that the information security officer (ISO) did not have consistent executive level support for obtaining authority to ensure that security initiatives were effectively implemented throughout the campus.

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. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program.

The interim CIO stated that the campus considered its organizational reporting structure to be consistent with that of the chancellor’s office, but he acknowledged that appropriate procedures to keep the president and cabinet informed and involved in information security on campus were not as robust as they could be.

Lack of appropriate oversight for the information security function could create conflicting priorities, lead to suppressed discoveries, and result in inadequate or conflicting budgetary decisions for projects.

Recommendation 1

We recommend that the campus ensure that information security initiatives are brought to the president’s cabinet regularly so that the vice presidents for each division are aware of and supportive of the implementation of information security initiatives.

Campus Response

We agree. The CIO will report on information security initiatives during the monthly luncheon for the president’s cabinet so that the vice presidents for each division are aware of and supportive of the implementation of such initiatives.

Documentation of the process will be provided by January 5, 2012.

INFORMATION SECURITY REPORTING

The process for reporting on information security incidents and initiatives needed improvement.
Specifically, we found that:

- The campus did not have a procedure to identify and report all security incidents, including those that occurred outside of the purview of information technology (IT) support services. Several campus computers were not provisioned or maintained by the campus IT department, and the departments supporting these computers did not consistently track security incidents or report them to the information security office.

- Security initiatives were not consistently reported to campus executive management. In addition, reporting of initiatives was sometimes incomplete, as it did not always specifically identify the status of critical projects that were delayed, nor did it provide a time frame for addressing such projects.

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 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.

The ISO stated that he did not have a method to ensure that security incidents that occurred outside of the purview of IT were reported, and he had not considered using the work order tracking system to compile reports of specific security events. He also stated that he provided executive reporting to the CIO, who was a member of the president’s council.

Incomplete compilation and tracking of security incidents prevents the ISO from ensuring that such breaches are handled appropriately, and failure to include inactive security projects in reports to executive management prevents campus management from understanding the overall exposure to information security threats and from providing input on priorities and funding for such projects.

**Recommendation 2**

We recommend that the campus:

a. Develop a procedure to identify and report all campus security incidents, including those that occur outside of the purview of IT support services.

b. Ensure that security initiatives are consistently reported to executive management, and that such reports are complete.

**Campus Response**

We agree.

a. The campus will develop a procedure for appropriate reporting of all information security incidents.
b. Security initiatives will be reported during the monthly luncheon for the president’s cabinet.

Documentation of the reporting process of security incidents and security initiatives will be provided by January 5, 2012.

**ASSET MANAGEMENT**

Several campus computers were not subject to information security oversight.

We found several campus computers that were not provisioned or maintained by the campus IT department. As a result, the information security office did not track, secure, and perform security monitoring on these computers.

ICSUAM §8065, *Information Asset Management*, 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 ISO stated that most state-owned equipment is controlled and secured by IT; however, certain departments procure equipment outside of the existing process, and therefore, the equipment is not always initially tracked, secured, and subsequently monitored.

Inadequate security over campus computing equipment, especially that which contains personal confidential information or has access to such protected information, increases the risk of loss and inappropriate use of state resources and increases campus exposure to information security breaches.

**Recommendation 3**

We recommend that the campus ensure that all campus computers are provisioned and maintained by the campus IT department, and that the information security office tracks, secures, and performs security monitoring on these computers.

**Campus Response**

We agree. The campus will ensure that campus-purchased computers are provisioned and maintained by the campus IT department with the assistance of formally approved/trained designees of selected departments (as appropriate). The information security office, with the assistance of the approved/trained designees, will track, secure, and perform necessary security monitoring on these computers.

Documentation of the implementation process will be provided by January 5, 2012.
NETWORK SECURITY

WIRELESS ENCRYPTION

Campus wireless networks were not configured to encrypt network traffic, and as a result, sensitive data accessed or transmitted by this communication method was not protected from threats or compromise.

ICSUAM §8045.100, Information Technology Security, 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 wireless network authentication had been encrypted, but that the campus had not yet encrypted wireless communication because other network initiatives had higher priority.

Inadequate control over wireless communication, especially when used to access sensitive information, increases the risk of loss and inappropriate use of such data and increases campus exposure to information security breaches.

Recommendation 4

We recommend that the campus encrypt all wireless networks so that sensitive data accessed and transmitted via campus wireless networks is appropriately protected.

Campus Response

We agree. Encryption methods have been developed and are now in place. Technical specifications illustrating the encryption of all wireless networks so that sensitive data accessed and transmitted via campus wireless networks is appropriately protected will be provided by January 5, 2012.

FIREWALL CONFIGURATION

Firewall filtering of inbound traffic from the Internet was not set to automatically deny potentially dangerous network traffic, and as a result, network devices and desktop computers were not fully protected against external attacks.

ICSUAM §8045, Information Technology Security, 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 had begun efforts to segment the internal network into separate security zones but had not yet completed the project because other network initiatives had higher
priority, and because of the significant effort needed to make sure that legitimate network services were not interrupted.

Failure to restrict unnecessary and often malicious network traffic from the public Internet increases the risk that campus equipment used to access sensitive data could be compromised.

**Recommendation 5**

We recommend that the campus set the firewall filtering of inbound traffic from the Internet to automatically deny potentially dangerous network traffic.

**Campus Response**

We agree. The campus will develop and implement a methodology to set up a firewall filtering of inbound traffic from the Internet to automatically deny potentially dangerous network traffic.

Documentation of the process will be provided by January 5, 2012.

**NETWORK SEGMENTATION**

The campus had not placed Internet-accessible web servers on a separate network segment from other internal production servers.

ICSUAM §8045.100, *Information Technology Security*, 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.

ICSUAM §8045.300, *Network Security*, states that campuses must appropriately design their networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity, and availability of their information assets. Each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

The ISO stated that the campus was in the process of segmenting the internal network into separate security zones but had not yet moved all Internet-facing servers into the proper security zone.

Failure to separate and protect internal resources from Internet-accessible devices increases the risk of internal network exposure to security compromises and inadequate security over information assets with protected data.
Recommendation 6

We recommend that the campus place Internet-accessible web servers on a separate network segment from other internal production servers.

Campus Response

We agree. The implementation has been completed.

Documentation of the process will be provided by January 5, 2012.

INFORMATION SECURITY AWARENESS TRAINING

Faculty members with access to student records were not required to complete information security awareness training.

ICSUAM §8035.100, Information Security Awareness and Training, 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.

The ISO stated that the CSU-sponsored security training had been provided to all campus employees, but that the campus organizational structure did not provide him with authority to enforce faculty participation.

Failure to provide all employees with information security awareness training increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

Recommendation 7

We recommend that the campus require that all employees with access to critical systems or protected data complete information security awareness training.

Campus Response

We agree. IT will run reports for all employees to track the completion of the information security awareness training (ISAT). A list of persons who fail to complete training ISAT training will be forwarded to the appropriate vice president for follow-up.
APPLICATION SYSTEM ACCESS

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

We found that employees from several campus departments, such as housing and the student health center, had unlimited access to all student grades.

ICSUAM §8060, Access Control, 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.

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

The Common Management System security administrator stated that he was uncertain as to why some of those groups had access to student grades. He stated his belief that it was the result of a conversion from the prior version of PeopleSoft.

Improper segregation of employee system access could lead to unauthorized or inappropriate exposure to sensitive data and can adversely affect campus compliance with existing regulations regarding protection of such data.

Recommendation 8

We recommend that the campus:

a. Appropriately restrict student grade information to authorized personnel.

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

Campus Response

We agree.

a. Access to grades has been restricted to authorized personnel.
b. An annual system access review process has been implemented.

Documentation of the actions will be provided by January 5, 2012.
# APPENDIX A:
PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ruben Armiñana</td>
<td>President</td>
</tr>
<tr>
<td>Brian Biggs</td>
<td>Analyst/Programmer, Information Technology</td>
</tr>
<tr>
<td>Barry Blackburn</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Brent Boyer</td>
<td>Associate Director, Disability Services</td>
</tr>
<tr>
<td>Brandon Dudley</td>
<td>Director, Library Technology</td>
</tr>
<tr>
<td>Peter Flores</td>
<td>Common Management System Security Administrator</td>
</tr>
<tr>
<td>Laurence Furukawa-Schlereth</td>
<td>Vice President of Administration and Finance</td>
</tr>
<tr>
<td>Andru Luvisi</td>
<td>Operating System Security Specialist</td>
</tr>
<tr>
<td>Roger Mamer</td>
<td>Systems Specialist, Computer Sciences</td>
</tr>
<tr>
<td>Robin Marshall</td>
<td>Director, Workstation Services and Security</td>
</tr>
<tr>
<td>Ruth McDonnell</td>
<td>Deputy Controller, Contracts and Procurement</td>
</tr>
<tr>
<td>Sally Sacchetto</td>
<td>Director of Faculty Personnel</td>
</tr>
<tr>
<td>Georgia Schwartz</td>
<td>Medical Director</td>
</tr>
<tr>
<td>Kathleen Spitzer</td>
<td>Managing Director, Employee Services</td>
</tr>
<tr>
<td>Jean Sugiyama</td>
<td>Network Analyst</td>
</tr>
<tr>
<td>Stephanie Thibault</td>
<td>Instructional Technology Technician, Biology</td>
</tr>
<tr>
<td>Jason Wenrick</td>
<td>Interim Chief Information Officer</td>
</tr>
<tr>
<td>Lisa Wyatt</td>
<td>Director of Counseling, Psychological Services</td>
</tr>
</tbody>
</table>
November 15, 2011

MEMORANDUM

TO: Larry Mandel  
University Auditor  
California State University  
401 Golden Shore, 4th Floor  
Long Beach, California 90802-4200

FROM: Laurence Furukawa-Gudereth  
Chief Financial Officer and  
Vice President for Administration and Finance

SUBJECT: Sensitive Data Security and Protection, Audit Report #11-50  
Campus Response

On behalf of President Armiñana, I am submitting the initial Campus Response to the recommendations of Audit Report # 11-50, Sensitive Data Security and Protection.

We will provide documentation to demonstrate the completion of corrective actions for each recommendation.

This memorandum [pdf copy], and the Campus Response is submitted via email to OUA@calstate.edu.

Enclosure

c: President Ruben Armiñana  
Andrew Rogerson  
Letitia Coate  
Jason Wenrick  
Andru Luvisi  
Brian Orr  
Kurt Koehle
SENSITIVE DATA SECURITY AND PROTECTION
SONOMA STATE UNIVERSITY
Audit Report 11-50

SECURITY GOVERNANCE

INFORMATION SECURITY ORGANIZATION

Recommendation 1

We recommend that the campus ensure that information security initiatives are brought to the president’s cabinet regularly so that the vice presidents for each division are aware of and supportive of the implementation of information security initiatives.

Campus Response

We agree. The Chief Information Officer will report on information security initiatives during the monthly luncheon for the president’s cabinet so that the vice presidents for each division are aware of and supportive of the implementation of such initiatives.

Documentation of the process will be provided by January 5, 2012.

INFORMATION SECURITY REPORTING

Recommendation 2

We recommend that the campus:

a. Develop a procedure to identify and report all campus security incidents, including those that occur outside of the purview of IT support services.

b. Ensure that security initiatives are consistently reported to executive management, and that such reports are complete.

Campus Response

We agree.

a. The campus will develop a procedure for appropriate reporting of all information security incidents.

b. Security initiatives will be reported during the monthly luncheon for the president’s cabinet.

Documentation of the reporting process of security incidents and security initiatives will be provided by January 5, 2012.
ASSET MANAGEMENT

Recommendation 3

We recommend that the campus ensure that all campus computers are provisioned and maintained by the campus IT department, and that the information security office tracks, secures, and performs security monitoring on these computers.

Campus Response

We agree. The campus will ensure that campus purchased computers are provisioned and maintained by the campus IT department with the assistance of formally approved/trained designees of selected departments (as appropriate). The information security office, with the assistance of the approved/trained designees, will track, secure, and perform necessary security monitoring on these computers.

Documentation of the implementation process will be provided by January 5, 2012.

NETWORK SECURITY

WIRELESS ENCRYPTION

Recommendation 4

We recommend that the campus encrypt all wireless networks so that sensitive data accessed and transmitted via campus wireless networks is appropriately protected.

Campus Response

We agree. Encryption methods have been developed and are now in place.

Technical specifications illustrating the encryption of all wireless networks so that sensitive data accessed and transmitted via campus wireless networks is appropriately protected will be provided by January 5, 2012.

FIREWALL CONFIGURATION

Recommendation 5

We recommend that the campus set the firewall filtering of inbound traffic from the Internet to automatically deny potentially dangerous network traffic.

Campus Response

We agree. The campus will develop and implement a methodology to set up a firewall filtering of inbound traffic from the Internet to automatically deny potentially dangerous network traffic.

Documentation of the process will be provided by January 5, 2012.
NETWORK SEGMENTATION

Recommendation 6

We recommend that the campus place Internet-accessible web servers on a separate network segment from other internal production servers.

Campus Response

We agree. The implementation has been completed.

Documentation of the process will be provided by January 5, 2012.

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 7

We recommend that the campus require that all employees with access to critical systems or protected data complete information security awareness training.

Campus Response

We agree. IT will run reports for all employees to track the completion of the information security awareness training (ISAT). A list of persons who fail to complete training ISAT training will be forwarded to the appropriate Vice-President for follow-up.

Documentation of the process will be provided by January 5, 2012.

APPLICATION SYSTEM ACCESS

Recommendation 8

We recommend that the campus:

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

Campus Response

We agree.

a. Access to grades has been restricted to authorized personnel.
b. An annual system access review process has been implemented.

Documentation of the actions will be provided by January 5, 2012.
December 8, 2011

**MEMORANDUM**

TO: Mr. Larry Mandel  
University Auditor

FROM: Charles B. Reed  
Chancellor

SUBJECT: Draft Final Report 11-50 on  
*Sensitive Data Security and Protection*,  
Sonoma State University

In response to your memorandum of December 8, 2011, I accept the response as submitted with the draft final report on *Sensitive Data Security and Protection*, Sonoma State University.

CBR/amd