

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**SAN MARCOS**

**Audit Report 09-41**  
**April 13, 2010**

---

**Members, Committee on Audit**

Melinda Guzman, Chair  
Raymond W. Holdsworth, Vice Chair  
Herbert L. Carter Carol R. Chandler  
Kenneth Fong Margaret Fortune  
George G. Gowgani William Hauck  
Henry Mendoza

---

**Staff**

University Auditor: Larry Mandel  
Senior Director: Michelle Schlack  
IT Audit Manager: Greg Dove

---

**BOARD OF TRUSTEES**  
**THE CALIFORNIA STATE UNIVERSITY**

---

# CONTENTS

Executive Summary ..... 1

Introduction..... 2

    Background ..... 2

    Purpose..... 3

    Scope and Methodology ..... 5

---

# OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance..... 7

System Development and Change Management ..... 7

    Web Application Development and Maintenance ..... 7

    Website Application Vulnerabilities ..... 8

Systems Security and Monitoring ..... 9

    Technical Vulnerabilities..... 9

    Operating Systems Vulnerabilities ..... 9

    Password Standards ..... 10

    Firewalls and Routing and Switching Devices ..... 10

## **APPENDICES**

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

---

## **ABBREVIATIONS**

CSU	California State University
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISMS	Information Security Management System
IT	Information Technology

---

## **EXECUTIVE SUMMARY**

As a result of a systemwide risk assessment conducted by the Office of the University Auditor, the Board of Trustees, at its January 2008 meeting, directed that *Information Security* be reviewed. The Office of the University Auditor had not previously reviewed *Information Security* as a separate subject area audit.

We visited the California State University, San Marcos campus from September 21, 2009, through November 6, 2009, 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 information security controls. 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 of information security in effect as of November 6, 2009, taken as a whole, were sufficient to meet the objectives stated below.

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 aspects of information security, but was designed to assess the controls over management, increase awareness, and recommend implementation for significant security topics that are prevalent in the California State University computing 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 [7]**

The campus did not remind separating employees of their ongoing legal responsibility for maintaining the security of protected data.

### **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [7]**

Programmers were not prohibited from changing production code. In addition, two application vulnerabilities existed on the website selected for testing.

### **SYSTEMS SECURITY AND MONITORING [9]**

Technical vulnerabilities existed on a variety of campus servers and on selected operating systems. The campus password practices were not consistently followed. In addition, firewalls and routing and switching devices were not always properly configured or adequately secured.

---

## INTRODUCTION

### **BACKGROUND**

State Administrative Manual Section 5300 states that information security means the protection of information and information systems, equipment, and people 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 Section 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, California Office of Information Security.

The California State University (CSU) *Information Security Policy*, dated August 2002, states that the Board of Trustees of the CSU is responsible for protecting the confidentiality of information in the custody of the CSU; the security of the equipment where this information is processed and maintained; and the related privacy rights of the CSU students, faculty, and staff concerning this information. It is also the collective responsibility of the CSU, its executives, and managers to ensure:

- ▶ The integrity of the data.
- ▶ The maintenance and currency of the applications.
- ▶ The preservation of the information in case of natural or manmade disasters.
- ▶ Compliance with federal and state regulations, including intellectual property and copyright.

It further states that campuses must have security policies and procedures that, at a minimum, implement information security, confidentiality practices consistent with these policies, and end-user responsibilities for the physical security of the equipment and the appropriate use of hardware, software, and network facilities. The policy applies to all data systems and equipment on campus that contain data deemed private or confidential and/or which contain mission critical data, including departmental, divisional, and other ancillary systems and equipment.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published an information security standard in 2005 as ISO/IEC 17799:2005 *Information Technology - Security Techniques - Code of Practice for Information Security Management*. This standard was subsequently renumbered as ISO/IEC 27002:2005 in July 2007 in order to bring it into line with the other ISO/IEC 27000-series standards, also known as the Information Security Management System (ISMS) Family of Standards. The ISMS Family of Standards comprises information security standards published jointly by the ISO and the IEC.

The CSU contracted with Unisys in 2006 to perform a series of on-site Information Security Assessment Reviews at nine campuses and the chancellor's office. This assessment was designed to perform a basic review of CSU information security as benchmarked against the industry-accepted standard, ISO 17799:2005, as well as all applicable state and federal laws.

The CSU also contracted with CH2MHill in 2007 for the development of comprehensive information security policies and standards. These policies and standards address the following areas: information security roles and responsibilities; risk management; acceptable use; personnel security; privacy; security awareness and training; third-party services security; information technology security; configuration management and change control; access control; asset management; management of information systems; information security incident management; physical security; business continuity and disaster recovery; and legal and regulatory compliance. The Information Technology Advisory Committee, composed of the chief information officers from each campus, and the Information Security Advisory Committee, composed of the information security officers from each campus, was integrally involved in this policy development process in order to ensure that the final product was an appropriate fit for the CSU. This project began in September 2007 with the expectation that these policies and standards were to be completed by August 2008 for subsequent adoption and official systemwide distribution in late 2008. This timeline has now been extended. Due to the pending status of this project during the time frame of the information security audits, these policies and standards were not used for evaluation of the campuses information security posture.

At California State University, San Marcos, the office of information technology services has overall responsibility for the management of campus systems and networks.

## **PURPOSE**

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration of information security and to determine the adequacy of controls over the related processes to evaluate adherence to an industry-accepted standard, ISO 17799/27002, *Code of Practice for Information Security Management*, 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, formation of 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 granted responsibility for maintenance and control to achieve and maintain appropriate protection of organizational assets; and information is appropriately classified to indicate the need, priorities, and expected degree of protection when handling the information.
- ▶ Security responsibilities are addressed prior to 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; and procedures are in place to ensure that users' separation from the organization is managed and that the return of all equipment and the removal of all access rights are completed.

- ▶ 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 networks, systems, applications, business processes, and data are controlled based on business and security requirements by means of user identification and authentication.
- ▶ Formal event reporting and escalation procedures are in place for information security events and weaknesses; and communication is accomplished in a consistent and effective manner, allowing timely corrective action to be taken.
- ▶ The design, operation, use, and management of information systems are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- ▶ Web application development and change management processes and procedures are adequate to ensure that application security and accessibility is considered during the design phase, that testing includes protection against known vulnerabilities, and that production servers are adequately protected.
- ▶ E-mail systems are properly configured and managed so that vulnerabilities are not allowed into the network, incidents are properly escalated, campus usage and retention guidelines are followed, and e-mail addresses are maintained in a central location to facilitate campus-wide communications.
- ▶ The operational security of selected operating systems is adequate to prevent the exploitation of vulnerabilities on the internal network by individuals who gain access to it from dial-in connections, the Internet, and hosts on the internal network.
- ▶ The Internet firewall system is sufficient to identify and thwart attacks from the external Internet and filter unwanted network traffic.
- ▶ Selected routing and switching devices are properly managed and configured to effectively provide the designated network security or traffic controls.
- ▶ Systems connected to the Internet make publicly available any information that may provide enticement to penetrate the Internet gateway.
- ▶ Web application vulnerabilities that provide the potential for an unauthorized party to subvert controls and gain access to critical and proprietary information, use resources inappropriately, interrupt business, or commit fraud are identified and addressed.

## **SCOPE AND METHODOLOGY**

The proposed scope of the audit, as presented in Attachment B, Audit Agenda Item 2 of the January 22-23, 2008, meeting of the Committee on Audit, stated that information security would include reviewing the systems and managerial/technical measures for ongoing evaluation of data/information collected; identifying confidential, private, or sensitive information; authorizing access; securing information; detecting security breaches; and evaluating security incident reporting and response. Information security includes the activities/measures undertaken to protect the confidentiality, integrity, and access/availability of information, including measures to limit collection of information, control access to data and assure that individuals with access to data do not utilize the data for unauthorized purposes, encrypt data in storage and transmission, and implement physical and logical security measures for all data repositories. Potential impacts include inappropriate disclosures of information; identity theft; adverse publicity; excessive costs; inability to achieve institutional objectives and goals; and increased exposure to enforcement actions by regulatory agencies.

In addition to the interviews and inquiry procedures affecting the operation and support of the network devices reviewed by the Office of the University Auditor, we also retained contractors to perform a technical security assessment that included running diagnostic software designed to identify improper configuration of selected systems, servers, and network devices. The purpose of the technical security assessment was to determine the effectiveness of technology and security controls governing the confidentiality, integrity, and availability of selected campus assets. The assessment contained an internal component (within the campus network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the California State University, San Marcos campus. Specifically, this configuration testing included assessment of the following technologies:

- ▶ Selected operating system platforms.
- ▶ Border firewall settings.
- ▶ Selected routing and switching devices.
- ▶ Internet footprint analysis.
- ▶ Website vulnerability assessment.

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 internal administrative, compliance, and operational/technical controls over the management of information security. 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, information processing, and service delivery.
- ▶ Access controls over networks, systems, applications, business processes, and data.
- ▶ Incident response, escalation, and reporting procedures.
- ▶ Compliance with relevant statutory, regulatory, and contractual security requirements.
- ▶ Web application security and applicable change management procedures.
- ▶ E-mail systems management and configuration.
- ▶ Operational security of selected operating system platforms.
- ▶ Security configurations of border firewall settings.
- ▶ Security configurations of selected routing and switching devices.
- ▶ Internet footprints of systems connected to the Internet.
- ▶ Website vulnerabilities stemming from exposures in the server's operating system, server administration practices, or flaws in the web application's programming.

Our testing and methodology was designed to provide a managerial level review of key information security practices, which included detailed testing of a limited number of network and computing devices. Our review did not examine all aspects of information security, selected emerging technologies were excluded from the scope of the review, and our testing approach was designed to provide a view of the security technologies used to protect only key computing resources.

---

## **OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES**

### **SECURITY GOVERNANCE**

The campus did not remind separating employees of their ongoing legal responsibility for maintaining the security of protected data.

The information security officer stated that the campus believed the confidentiality agreement informed employees of their legal responsibility to maintain the security and privacy of protected information. She further stated that the campus was not aware that it needed to include a reminder in the employee separation process.

Failure to notify separating employees of their ongoing legal responsibility to maintain the security of protected data increases the risk that they will not comply with statutory information security requirements for any remaining access to, or unauthorized custody of, protected data.

#### **Recommendation 1**

We recommend that the campus include in its personnel exit process a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

#### **Campus Response**

We concur. The campus will alter its personnel exit process to include a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data by August 31, 2010.

### **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

#### **WEB APPLICATION DEVELOPMENT AND MAINTENANCE**

The web application development and change management practices required improvement.

Specifically we noted that programmers were not prohibited from changing production code.

The director of system development and software engineering stated that the existing process provided for management review of authorized changes; however, the process did not include the monitoring of unauthorized changes.

The lack of a sufficient web application development control process increases the risk that web application changes may be unauthorized and may be inconsistent with user and management expectations.

### **Recommendation 2**

We recommend that the campus restrict developers' ability to move web application changes into production, or create a procedure so that management monitors changes to production.

### **Campus Response**

We concur. The campus will alter its web application development practices to include steps to monitor the state of production code in order to avoid unauthorized changes by August 31, 2010.

## **WEBSITE APPLICATION VULNERABILITIES**

Two application vulnerabilities existed on the website selected for testing.

The director of system development and software engineering stated that the campus was improving its process continuously to identify and correct vulnerabilities as they occurred, but had not yet considered those identified in the audit.

Web application vulnerabilities increase the risk that a remote attacker may be able to access protected confidential information or execute malicious programs on the server that could disable other network resources.

### **Recommendation 3**

We recommend that the campus:

- a. Repair the website vulnerabilities that were identified and presented in detail.
- b. Implement a process for periodic scanning of existing web applications to minimize its potential susceptibility to new vulnerabilities.

### **Campus Response**

We concur. The campus has repaired the website vulnerability identified in the audit. The campus will implement a process for periodic scanning of web applications by August 31, 2010.

## **SYSTEMS SECURITY AND MONITORING**

### **TECHNICAL VULNERABILITIES**

Technical vulnerabilities existed on a variety of campus servers.

Our testing of selected servers disclosed five for which specific details were provided to the campus.

The information security officer stated that some of the vulnerabilities were a result of the timing of the audit in relation to their patching process and that the rest of the items were considered lower risk and had not been removed from some of the servers examined.

Server vulnerabilities increase the risk of a security breach that could compromise the server and possibly result in loss of protected confidential information or allow the execution of malicious programs that could adversely affect other network resources.

#### **Recommendation 4**

We recommend that the campus repair all of the technical vulnerabilities that were identified and presented in detail.

#### **Campus Response**

We concur. The campus has repaired the technical vulnerabilities identified in the audit. Where vulnerabilities result from application configuration, we will institute a process of periodic risk analysis of the application configuration by August 31, 2010.

### **OPERATING SYSTEMS VULNERABILITIES**

Technical vulnerabilities existed on selected operating systems.

Our testing of selected servers disclosed various vulnerabilities for which specific details were provided to the campus.

The information security officer stated that the vulnerabilities identified represented low risk and that the file-level security procedure would be examined to ensure that new files are created with appropriate security.

These vulnerabilities increase the risk of a remote attack that could lead to loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

### **Recommendation 5**

We recommend that the campus repair all the technical vulnerabilities that were identified and presented in detail.

### **Campus Response**

We concur. The campus has repaired the technical vulnerabilities identified in the audit. The campus will institute a periodic review of file permissions on shared servers to ensure that they are accurately assigned by August 31, 2010.

## **PASSWORD STANDARDS**

The campus password practices were not consistently followed.

We noted that 20 of 24 user accounts had non-expiring passwords on one server and two servers did not enforce password standards that are consistent with campus policy.

The information security officer stated that the campus had been making significant changes to the network environment, but had not recently revisited the password policies on the existing systems.

The lack of a standard enforced password policy for critical applications increases the risk of easily guessed passwords and possible unauthorized access to network resources and confidential information.

### **Recommendation 6**

We recommend the campus extend its password policy to all servers and network devices and implement procedures to ensure compliance with the policy.

### **Campus Response**

We concur. The campus will implement policies to ensure that all servers and network devices comply with the appropriate password policy by August 31, 2010.

## **FIREWALLS AND ROUTING AND SWITCHING DEVICES**

Firewalls and routing and switching devices were not always properly configured or adequately secured.

Our testing of selected network devices disclosed various vulnerabilities for which specific details were provided to the campus.

The information security officer stated that the campus had not consistently implemented password-naming conventions on all network devices.

These vulnerabilities increase the risk that a remote attacker may be able to exploit network resources, gain access to protected confidential information, or execute malicious programs that could potentially disable other network resources.

**Recommendation 7**

We recommend that the campus repair the network device vulnerabilities that were identified and presented in detail.

**Campus Response**

We concur. The campus has repaired the technical vulnerabilities identified in the audit, and will provide documentation of repairs by August 31, 2010.

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Karen S. Haynes	President
Tyson Bizzigotti	Analyst Programmer
Wanda Boller	Manager, Human Resources
Marina Christensen	Analyst Programmer
Bill Craig	Lead, Enterprise Systems
Garrett Collins	Information Technology Consultant, User Support Services
Wayne Dilly	Operating Systems Analyst, Enterprise Systems
Jon Fischer	Operating Systems Analyst, Enterprise Group
Vincent Gray	Lead Network Analyst, Telecommunications and User Support Services
Linda Hawk	Vice President, Finance and Administrative Services
Jeff Henson	Analyst Programmer, Systems Development and Software Engineering
John Humes	Network Analyst
Becky Hunt	Systems Development Analyst
Mike Irick	Technology Strategist Coordinator
Margo Lopez	Director, System Development and Software Engineering
Teresa Macklin	Information Security Officer
David Medeiros	Senior Systems Engineer, Enterprise Systems
Diane Peterson	Systems Architect and DBA, Systems Development
Katy Rees	Director, Strategic Planning and Administrative Services
Barbara Sadnick	Administrative Support Assistant
Wayne Veres	Chief Information Officer
Jeremy Villegas	Network Analyst, Telecommunications and User Support Services
Bill Ward	Associate Dean
Michael Yee	System Security Auditor



April 19, 2010

Mr. Larry Mandel  
University Auditor  
The California State University  
401 Golden Shore  
Long Beach, CA 90802

RECEIVED  
UNIVERSITY AUDITOR

APR 21 2010

THE CALIFORNIA STATE  
UNIVERSITY

Subject: Campus Response to Audit Report 09-41, Information Security  
California State University San Marcos

Dear Mr. Mandel:

Enclosed is our campus response to the seven recommendations in Audit Report 09-41, Information Security. We anticipate sending our supporting evidence no later than August 31, 2010.

Please let us know if you have any questions or need additional information.

Sincerely,

Linda Hawk  
Vice President  
Finance and Administrative Services

Enclosures

cc: President Karen S. Haynes

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**SAN MARCOS**

**Audit Report 09-41**

**SECURITY GOVERNANCE**

**Recommendation 1**

We recommend that the campus include in its personnel exit process a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

**Campus Response**

We concur. The campus will alter its personnel exit process to include a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data by August 31, 2010.

**SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

**WEB APPLICATION DEVELOPMENT AND MAINTENANCE**

**Recommendation 2**

We recommend that the campus restrict developers' ability to move web application changes into production, or create a procedure so that management monitors changes to production.

**Campus Response**

We concur. The campus will alter its web application development practices to include steps to monitor the state of production code in order to avoid unauthorized changes by August 31, 2010.

**WEBSITE APPLICATION VULNERABILITIES**

**Recommendation 3**

We recommend that the campus:

- a. Repair the website vulnerabilities that were identified and presented in detail.
- b. Implement a process for periodic scanning of existing web applications to minimize its potential susceptibility to new vulnerabilities.

**Campus Response**

We concur. The campus has repaired the website vulnerability identified in the audit. The campus will implement a process for periodic scanning of web applications by August 31, 2010.

**SYSTEMS SECURITY AND MONITORING**

**TECHNICAL VULNERABILITIES**

**Recommendation 4**

We recommend that the campus repair all of the technical vulnerabilities that were identified and presented in detail.

**Campus Response**

We concur. The campus has repaired the technical vulnerabilities identified in the audit. Where vulnerabilities result from application configuration, we will institute a process of periodic risk analysis of the application configuration by August 31, 2010.

**OPERATING SYSTEMS VULNERABILITIES**

**Recommendation 5**

We recommend that the campus repair all the technical vulnerabilities that were identified and presented in detail.

**Campus Response**

We concur. The campus has repaired the technical vulnerabilities identified in the audit. The campus will institute a periodic review of file permissions on shared servers to ensure that they are accurately assigned by August 31, 2010.

**PASSWORD STANDARDS**

**Recommendation 6**

We recommend the campus extend its password policy to all servers and network devices and implement procedures to ensure compliance with the policy.

**Campus Response**

We concur. The campus will implement policies to ensure that all servers and network devices comply with the appropriate password policy by August 31, 2010.

## **FIREWALLS AND ROUTING AND SWITCHING DEVICES**

### **Recommendation 7**

We recommend that the campus repair the network device vulnerabilities that were identified and presented in detail.

### **Campus Response**

We concur. The campus has repaired the technical vulnerabilities identified in the audit, and will provide documentation of repairs by August 31, 2010.



THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR

BAKERSFIELD

May 5, 2010

CHANNEL ISLANDS

CHICO

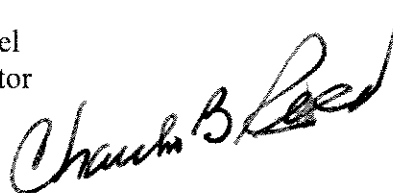
**MEMORANDUM**

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FROM: Charles B. Reed  
Chancellor


FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 09-41 on *Information Security*,  
California State University, San Marcos

LONG BEACH

LOS ANGELES

In response to your memorandum of May 5, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, San Marcos.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS