

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
LOS ANGELES

Audit Report 09-42
April 6, 2010

Members, Committee on Audit

Henry Mendoza, Chair
Raymond W. Holdsworth, Vice Chair
Nicole M. Anderson Margaret Fortune
George G. Gowgani Melinda Guzman
William Hauck

Staff

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

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary 1

Introduction..... 3

 Background 3

 Purpose..... 4

 Scope and Methodology 6

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance..... 8

Decentralized Computing 9

Systems Security and Monitoring..... 9

 Firewalls and Routing and Switching Devices 9

 Operating Systems Vulnerabilities 10

 Review of Security Event Logs 10

 Control of User Access 11

 Assessment of Protected Information 12

APPENDICES

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

ABBREVIATIONS

CMS	Common Management Systems
CSU	California State University
CSULA	California State University, Los Angeles
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
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 Los Angeles campus from November 9, 2009, through December 16, 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 December 16, 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 [8]

The campus had not finalized and communicated information security policies.

DECENTRALIZED COMPUTING [9]

Technical vulnerabilities existed on a variety of systems throughout the campus.

SYSTEMS SECURITY AND MONITORING [9]

Firewalls and routing and switching devices were not always properly configured or adequately secured. Technical vulnerabilities existed on selected operating systems. The campus lacked a formal process for the review of security event logs. Administration of user access to certain decentralized systems and

applications containing protected data was inadequate. Laptops, desktops, or removable media containing sensitive information were not always encrypted.

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 (IT) 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, Los Angeles (CSULA), the office of information technology services has overall responsibility for the management of campus systems and networks. However, a significant level of decentralization has shifted many critical IT responsibilities to ancillary departmental units throughout the campus.

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 CSULA 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.

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.
- ▶ 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.

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 had not finalized and communicated information security policies.

We found that many campus information security policies were in draft form and pending formal approval.

The following policies/procedures were only available in draft form:

- Information Classification, Handling and Disposal
- Managing IT Systems and Network Operations
- User Guidelines for Information Security Contract Language
- Record Management Disposition Program
- User Guidelines for Teleworking
- User Guidelines for Mobile Computing
- User Guidelines for Responsible Use of Computing, Communications and Information Resources
- Campus Security Incident Response Team
- Information Technology Services Internal Procedures for Sanitization
- User Guidelines for Data Sanitation
- Password Standards

The director of information technology (IT) security and compliance stated that the review cycle and number of individuals, departments, and groups required to review and approve policies and procedures makes for a lengthy approval process before they are finalized and published.

Failure to finalize and communicate campus-wide policy increases the risk of unauthorized exceptions and could compromise compliance with statutory information security requirements. Such inaction also impacts the ability of the campus to evaluate the overall effectiveness of existing security provisions related to protected data.

Recommendation 1

We recommend that the campus finalize and communicate the above-noted information security policies and ensure that all departments comply with these policies.

Campus Response

The campus management and executives will continue to push forward the review and finalization of the information security policies and communicate and publish them for the campus community. The anticipated completion date is September 30, 2010.

DECENTRALIZED COMPUTING

Technical vulnerabilities existed on a variety of systems throughout the campus.

Our external testing of selected servers disclosed 32 vulnerabilities on a variety of servers. We provided specific details of these vulnerabilities to the campus.

The director of IT infrastructure stated that these vulnerabilities were caused by various factors, including some that have other mitigating controls, and routine delays in patching servers that are actively monitored by the campus IT department.

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

Recommendation 2

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

Campus Response

Mitigating controls have been implemented and the issues identified have been resolved.

SYSTEMS SECURITY AND MONITORING

FIREWALLS AND ROUTING AND SWITCHING DEVICES

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

Our testing of these devices disclosed six vulnerabilities. We provided details of these vulnerabilities to the campus.

The director of IT infrastructure stated that one of these vulnerabilities was attributed to staff oversight and the rest were due to requirements set forth by the chancellor's office standard operating environment for all of the California State University campuses.

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 3

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

Campus Response

Mitigating controls have been implemented and the issues identified have been resolved.

OPERATING SYSTEMS VULNERABILITIES

Technical vulnerabilities existed on operating systems selected for testing.

Our testing of three servers disclosed 13 various vulnerabilities. We provided details of these vulnerabilities to the campus.

The director of IT infrastructure stated that these vulnerabilities were caused by a number of various factors that included the timing of the external review of the servers, which was right after Microsoft released a number of patches that the campus was reviewing and testing to be issued during the next routine scheduled patch update cycle.

The vulnerabilities on these critical servers increases the risk of a remote attack that could result in a loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

Recommendation 4

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

Campus Response

The vulnerabilities identified were corrected during the normal monthly patch cycle.

REVIEW OF SECURITY EVENT LOGS

The campus lacked a formal process for the review of security event logs.

The director of IT infrastructure stated that the campus has a central system to retain logs that were reviewed only when necessary for incident response and forensics analysis.

The lack of periodic documented reviews of security event logs increases the risk that malicious activity could go undetected or viruses or other malicious code could be embedded within the campus network and its resources. This could lead to an unreported breach of confidential information.

Recommendation 5

We recommend that the campus implement the security log monitoring tool to centralize all security monitoring and provide trend analysis, logging, and automated notification.

Campus Response

The campus recently purchased a log management system that will be installed and will provide more extensive log analysis. Once installed, a process for reviewing reports will be defined. The anticipated completion date is August 31, 2010.

CONTROL OF USER ACCESS

Administration of user access to certain decentralized systems and applications containing protected data was inadequate.

We found that for two departmental systems:

- ▶ The campus did not consistently document the process for adding and removing user access.
- ▶ The campus did not consistently perform periodic management review and validation of system access and/or permissions.

The director of IT security and compliance stated that the two departmental systems reviewed were not part of the centrally managed administrative systems and did not follow the same stringent user access requirements.

Failure to adequately administer and monitor user account access privileges increases the risk of inappropriate access.

Recommendation 6

We recommend that the campus:

- a. Establish a documented process for adding and removing user accounts to decentralized systems.
- b. Perform and document periodic management reviews of user access privileges for all systems and applications containing protected data.

Campus Response

A procedure will be developed for those decentralized systems identified to ensure that user access is reviewed and documented. The anticipated completion date is August 31, 2010.

ASSESSMENT OF PROTECTED INFORMATION

Laptops, desktops, or removable media containing sensitive information were not always encrypted.

The director of IT security and compliance stated that per campus policy, departments and users are instructed to encrypt all protected data, and this may not have occurred in all instances.

Failure to effectively administer protected data on decentralized computers increases the risk that the computers may be compromised, resulting in potential loss of confidential data in the event of a security breach.

Recommendation 7

We recommend that the campus ensure encryption is used when sensitive information is stored on laptops, desktops, or removable media.

Campus Response

The campus will finalize the guideline for Information Classification, Handling and Disposal and publish and communicate to the campus community. The anticipated completion date is September 30, 2010.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
James M. Rosser	President
Yolanda Aguiar	Employee Relations Coordinator, Human Resources Management
Laura Carlson-Weiner	Director, Advancement Services
Bryant Chan	Information Technology Consultant, Office of Academic Affairs
Bill Chang	Director, CMS and Enterprise System
David Chang	Information Technology Coordinator, Office of Academic Affairs
Lisa Chavez	Associate Vice President, Administration and Finance (At time of review)
Kevin Chua	Information Technology Consultant, Student Affairs
Annie Ekshian	Administrative Analyst/Specialist, Business Financial Services
Gilbert Garcia	Information Technology Consultant, Office of Academic Affairs
Tanya Ho	University Internal Auditor
Bob Hoffman	Assistant Director, Network Operations Servers and Technology Operations
Monica Jazzabi	Acting Director, Student Health Center
Christine Leung	Senior Internal Auditor
Thomas Leung	University Controller, Business Financial Services
Sal Membreno	Director, Office of Academic Support
Sheryl Okuno	Director of IT Security and Compliance
Tom Ong	Information Systems Consultant
Peter Quan	Vice President, Information Technology Services
George Pardon	Vice President, Administration and Finance (At time of review)
Jae Park	Information Technology Consultant, Office of Academic Affairs
Chris Rapp	Director of IT Infrastructure
Lisa M. Sanchez	Director, Human Resources Management
Matt Warren	Divisional Fiscal Resource Manager



CALIFORNIA STATE UNIVERSITY, LOS ANGELES

OFFICE OF THE PRESIDENT

June 16, 2010

RECEIVED
UNIVERSITY AUDITOR

JUN 21 2010

THE CALIFORNIA STATE
UNIVERSITY

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

Re: *University's Response to Recommendations Contained in Report Number 09-42
Information Security Audit*

Dear Mr. Mandel:

Attached are the University's responses to the recommendations contained in Report Number 09-42, Information Security Audit.

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

Sincerely,

James M. Rosser
President

Attachment

cc: (with attachments)
Lisa Chavez, Interim Vice-President for Administration and Chief Financial Officer
Peter Quan, Vice-President for Information Technology Services
Sheryl Okuno, Director of IT Security and Compliance
Tanya Ho, University Internal Auditor
Jill Carnahan, University Compliance Officer

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
LOS ANGELES

Audit Report 09-42

SECURITY GOVERNANCE

Recommendation 1

We recommend that the campus finalize and communicate the above-noted information security policies and ensure that all departments comply with these policies.

Campus Response

The campus management and executives will continue to push forward the review and finalization of the information security policies and communicate and publish them for the campus community. The anticipated completion date is September 30, 2010.

DECENTRALIZED COMPUTING

Recommendation 2

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

Campus Response

Mitigating controls have been implemented and the issues identified have been resolved.

SYSTEMS SECURITY AND MONITORING

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 3

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

Campus Response

Mitigating controls have been implemented and the issues identified have been resolved.

OPERATING SYSTEMS VULNERABILITIES

Recommendation 4

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

Campus Response

The vulnerabilities identified were corrected during the normal monthly patch cycle.

REVIEW OF SECURITY EVENT LOGS

Recommendation 5

We recommend that the campus implement the security log monitoring tool to centralize all security monitoring and provide trend analysis, logging, and automated notification.

Campus Response

The campus recently purchased a log management system that will be installed and will provide more extensive log analysis. Once installed, a process for reviewing reports will be defined. The anticipated completion date is August 31, 2010.

CONTROL OF USER ACCESS

Recommendation 6

We recommend that the campus:

- a. Establish a documented process for adding and removing user accounts to decentralized systems.
- b. Perform and document periodic management reviews of user access privileges for all systems and applications containing protected data.

Campus Response

A procedure will be developed for those decentralized systems identified to ensure that user access is reviewed and documented. The anticipated completion date is August 31, 2010.

ASSESSMENT OF PROTECTED INFORMATION

Recommendation 7

We recommend that the campus ensure encryption is used when sensitive information is stored on laptops, desktops, or removable media.

Campus Response

The campus will finalize the guideline for Information Classification, Handling and Disposal and publish and communicate to the campus community. The anticipated completion date is September 30, 2010.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

August 12, 2010

CHICO

MEMORANDUM

DOMINGUEZ HILLS

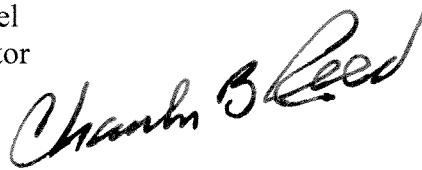
EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report 09-42 on *Information Security*,
California State University, Los Angeles

LONG BEACH

LOS ANGELES

In response to your memorandum of August 12, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, Los Angeles.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS