

INFORMATION SECURITY

**CALIFORNIA POLYTECHNIC STATE UNIVERSITY,
SAN LUIS OBISPO**

**Audit Report 09-40
April 21, 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
Internal Auditor: Salvador Rodriguez

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	4
Background	4
Purpose.....	5
Scope and Methodology	7

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance.....	9
Information Security Policy	9
Record Retention.....	9
Information Security Awareness Training.....	10
Information Security Plan	11
Security Authority and Responsibility	12
Information Security Management.....	13
Decentralized Computing	14
Server Environments	14
E-Mail Systems	15
Technical Vulnerabilities	16
System Development and Change Management	17
Systems Security and Monitoring.....	19
Control Over User Access.....	19
Password Standards.....	20
Network Architecture	20
Baseline Security Standards.....	21
Vulnerability Management.....	22
Review of Security Event Logs.....	22
Network Access.....	23
Threat Management.....	24
Configuration Changes.....	24
Granting Administrative Access	25
Firewalls and Routing and Switching Devices	26
Protected Data.....	27
Assessment and Inventory of Protected Information	27
System Backup Encryption	28
Incident Response Management.....	29
Disposition of Protected Data	30
Lost/Stolen Computers.....	31
Use of Employee-Owned Computers	32

APPENDICES

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

ABBREVIATIONS

CSU	California State University
EO	Executive Order
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Technology Services
LAN	Local-Area Network
SNMP	Simple Network Management Protocol
Telnet	Telecommunication Network
USB	Universal Serial Bus

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 Polytechnic State University, San Luis Obispo campus from September 21, 2009, through November 6, 2009, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, would continuously impact the overall control environment. We identified a series of problems that were listed individually in this report; however, the underlying root cause of many of the problems identified was the overall organization of information technology (IT) services using a decentralized campus computing environment that was not consistently managed in the same professional manner as the services provided by the campus IT department. Also, the campus environment did not lend itself to timely creation and issuance of campus-wide IT policies.

In our opinion, the operational and administrative controls of information security in effect as of November 6, 2009, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the campus IT department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems, the decentralized computing environments that were not under the purview of campus IT require significant improvement and management oversight.

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 [9]

The campus had not updated its information security policies to address the changing campus information technology environments(s) and recent statutory compliance requirements. The campus record retention action plan required improvement. Security awareness training had not been completed by all campus personnel with computer access. The campus' information security plan did not prioritize information security risks and include projected timelines for addressing information security issues.

The campus did not have a full-time information security officer, nor was management oversight provided to personnel with information security responsibilities. The campus had not appropriately defined the position and authority of the information security officer. The campus had not exercised oversight consistently over, nor enforced campus information security policies on the decentralized computing environments. Security responsibilities had not been formalized consistently, and the campus lacked position descriptions for campus-wide information technology personnel.

DECENTRALIZED COMPUTING [14]

Administration of decentralized departmental server environments required improvement. Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the campus IT team and were not held to the same programming standard, code review, or security configuration standards. The campus had not developed policies and procedures for the multiple e-mail systems used by decentralized departments.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [17]

Change management procedures for web application and development required improvement. The campus lacked a formal process to test for vulnerabilities in Web applications prior to their deployment into the production environment.

SYSTEM SECURITY AND MONITORING [19]

Administration and management of user access profiles required improvement. The campus password standards required improvement for centralized and decentralized computing environments. Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources. Baseline security standards for the administration for centralized and decentralized servers and desktops had not been developed. The campus did not have a process for detecting vulnerabilities related to the security of servers and desktops connected to the campus network. The campus lacked a formal process for the review of security event logs. The management of network and telecommunication devices attached to the network required improvement. The campus did not actively monitor intrusion security events. The campus lacked policies and procedures that defined a formal periodic review of configuration changes. The campus lacked a formal process for granting and managing privileged system-level access to accounts. Firewalls and routing and switching devices were not always properly configured or adequately secured, and the campus did not adequately secure the campus local area network.

PROTECTED DATA [27]

The campus had not completed a campus-wide assessment to identify sensitive data on all servers and workstations, and it did not have a formal process to identify, approve, or review access to confidential information owned and managed by campus ancillary sites. The campus had not finalized a data classification and handling policy. Protected data stored on laptops, external hard drives, and USB flash drives were not encrypted. The campus incident response process and procedures required improvement.

EXECUTIVE SUMMARY

The campus could not provide evidence documenting the deletion of protected data from campus computers. The campus asset management system did not track computer equipment procured for less than \$500 that stored protected data. The campus lacked a formal process to ensure that lost or stolen computers were properly reported to the information security officer to determine the disposition of sensitive information on computers and whether further action was required. The campus lacked a policy to address the use of employee-owned and/or non-state computers with access to campus resources.

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 Polytechnic State University, San Luis Obispo, 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 California Polytechnic State University, San Luis Obispo 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

INFORMATION SECURITY POLICY

The campus had not updated its information security policies to address the changing campus information technology (IT) environment(s) and recent statutory compliance requirements.

The director of technology services, administration and finance/information security officer stated that the campus had been waiting for the draft California State University (CSU) systemwide information security policies to be approved by the CSU so that they could be adopted on the campus.

Failure to properly update information security policies limits the effectiveness of information security governance and increases the risk of misunderstandings regarding user responsibilities.

Recommendation 1

We recommend that the campus update its information security policies to address the changing campus IT environments(s) and recent statutory compliance requirements.

Campus Response

We concur. The campus will update its information security policies by October 8, 2010.

RECORD RETENTION

The campus had not completed an assessment of its compliance with Executive Order (EO) 1031.

During our review of record retention practices, we noted that:

- ▶ One department had not completed the annual review of records.
- ▶ One department did not have formal procedures for record retention and disposition.
- ▶ Various departments had not completed record retention schedules.
- ▶ Record retention schedules were not developed for the disposition of e-mail. We noted that e-mail was retained for an indefinite period of time.

The director of technology services, administration and finance/information security officer stated that various campus departments have not finalized their record retention schedules and addressed other EO 1031 requirements due to competing priorities. Also, the information technology policy assurance officer stated that the campus had been waiting for direction to establish an e-mail retention policy from the CSU Information Technology Advisory Committee's e-mail retention project.

Failure to comply with EO 1031 increases the risk of inappropriate and untimely disposal of records/information. An excessive retention of e-mail could impact the campus should it be required to produce such documents for legal disclosure.

Recommendation 2

We recommend that the campus:

- a. Complete a record retention action plan and corresponding procedures that ensure its appropriate and timely disposal of records/information in accordance with campus time frames.
- b. Develop and document an e-mail retention policy.

Campus Response

We concur.

- a. The campus will prepare a record retention action plan to ensure its appropriate and timely disposal of records/information in accordance with campus time frames by October 8, 2010.
- b. The campus will develop and document an e-mail retention policy by October 8, 2010.

INFORMATION SECURITY AWARENESS TRAINING

Security awareness training had not been completed by all campus personnel with computer access.

The director of technology services, administration and finance/information security officer stated that the campus had implemented the CSU Workplace Answers security awareness web-based training program. She further stated that the campus does not have a formal information security awareness training policy requiring all employees to complete the training. She added that the campus had been awaiting approval of the draft systemwide CSU information security policies that included a security awareness training requirement.

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

Recommendation 3

We recommend that the campus develop a security awareness training policy and ensure that all employees with access to campus computing resources complete the training.

Campus Response

We concur. The campus will develop a security awareness training program to ensure that all employees with access to campus computing resources complete the training by October 8, 2010.

INFORMATION SECURITY PLAN

Administration of the campus information security program required improvement.

Specifically, we noted that:

- ▶ Although the campus was using an informal risk assessment, a formal information security risk assessment had not been conducted.
- ▶ The information security plan did not prioritize all information security risks nor had a timeline for addressing the risks been established.

The director of technology services, administration and finance/information security officer stated that although the campus had previously performed a risk assessment, it had not updated this assessment to address current risks.

The lack of a formal risk assessment process to identify and prioritize information security risks and create a formal action plan to adequately address identified risks within an established timeline increases the potential for misunderstandings regarding campus information security policy. This also impacts the campus' ability to evaluate the overall effectiveness of existing security provisions for protected data.

Recommendation 4

We recommend that the campus:

- c. Conduct a formal information security risk assessment.
- d. Update the plan to prioritize all information security risks and establish specific timelines for addressing the risks.

Campus Response

We concur. The campus will update its information security risk assessment with updated risks by October 8, 2010. The campus has completed update of the plan with assigned priorities and timelines for addressing the risks.

SECURITY AUTHORITY AND RESPONSIBILITY

The overall information security authority and responsibility designations required improvement.

We noted that:

- ▶ The campus did not provide sufficient management oversight to personnel with information security responsibilities
- ▶ The campus had not formally recognized the information security officer's respective responsibilities and authorities. The campus had not granted the information security officer the authority to establish operational information security procedures.
- ▶ The campus had not provided the information security officer with a formal delegation of authority to oversee and enforce campus information security policies and procedures, nor did it provide the information security officer with a formal delegation of authority to coordinate information security efforts across the university to facilitate effective compliance efforts.
- ▶ Security responsibilities had not been adequately defined in the job/position descriptions of campus-wide IT personnel that manage various computing environments.

The director of technology services, administration and finance/information security officer stated that the campus had appointed an information security officer, but authority to create information security policies, procedures, and assign security responsibilities to campus employees resided with the campus Information Resource Management Policy and Planning Committee that was chaired by the campus vice provost of information technology/chief information Officer.

The lack of a full-time information security officer limits the campus' ability to direct a comprehensive system of information security. It also hinders the campus' ability to apply security governance consistently and to prioritize information security initiatives.

Recommendation 5

We recommend that the campus:

- a. Provide sufficient management oversight to ensure that security responsibilities are being addressed by the departmental and college information security designees.
- b. Formally define and communicate the information security officer's roles, responsibilities, and authority.
- c. Formalize position/job descriptions to include security responsibilities for designated information technology personnel.

Campus Response

We concur.

- a. The campus will develop a process to monitor departmental and college information security designee's technology environments annually by October 21, 2010.
- b. The campus will update and communicate the information security officer's roles, responsibilities, and authorities in the updated information security program by October 21, 2010.
- c. The campus will define security responsibilities for designated IT personnel to update their job descriptions by October 21, 2010.

INFORMATION SECURITY MANAGEMENT

The monitoring and enforcement of campus-wide information security policies and standards were deficient.

We found that the central information technology services (ITS) department had not exercised consistent oversight, nor had it enforced the existing campus information security policies and procedures on the decentralized computing environments to ensure compliance.

The director of technology services, administration and finance/information security officer stated that the decentralized computing environments' non-compliance with campus information security policies was due to a lack of coordination between colleges and the central ITS department. She further stated that the lack of training and updated security procedures contributed to the non-compliance of the decentralized computing environments with campus information security policies.

Failure to monitor and enforce campus-wide policies and standards limits the campus' ability to direct a comprehensive information security program. Such oversights increase the campus' exposure to security breaches and the risk of inappropriate use of computing resources.

Recommendation 6

We recommend that the campus:

- a. Develop a process to track and report on the various decentralized computing environments' ongoing compliance with campus information security policies and procedures.
- b. Ensure that relevant campus and college IT staff are adequately trained on their newly defined security responsibilities and procedures.

Campus Response

We concur.

- a. The campus will develop a process to monitor departmental and college information security designee's technology environments annually by October 21, 2010.
- b. The campus will implement a training plan for campus and IT staff on information security policies, standards, and guidelines by October 21, 2010.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Administration of decentralized departmental server environments required improvement.

Our review of the decentralized computing environments disclosed that:

- ▶ Three out of nine decentralized environments reviewed did not follow the campus information security policies and procedures.
- ▶ Various decentralized IT environments had not formalized patch management procedures to ensure that the most current virus definitions and vendor software patches were installed.
- ▶ The employees of various colleges and departments managed their own servers/desktop computers and were not monitored to ensure adequate patch management, antivirus updates, and minimum security baseline standards.
- ▶ The campus did not adequately control the administration of privileged users' accounts, nor did it adequately monitor their access to systems and applications.

The director of technology services, administration and finance/information security officer stated that the decentralized departments are responsible for the management of their server environments but that there had been no oversight to ensure that the departments consistently followed best practices.

Failure to effectively administer decentralized servers increases the risk that the servers may be compromised, resulting in potential loss of confidential data in the event of a security breach, and contributes to inefficient use of campus resources.

Recommendation 7

We recommend that the campus:

- a. Formally communicate campus-wide information security policies and procedures and enforce compliance in decentralized computing environments.
- b. Ensure that the departments' patch management processes are sufficient to guarantee that the most current software patches are installed in a timely manner.
- c. Eliminate administrative access to computers unless specifically approved.
- d. Ensure that decentralized IT professionals in the colleges and departments have appropriate authority and oversight over information security practices in their computing environments.

Campus Response

We concur.

- a. The campus will formally communicate its information security policies, standards, and guidelines to the campus IT staff by November 30, 2010. The campus will develop a process to monitor and enforce compliance in the decentralized computing environments by November 30, 2010.
- b. The campus will develop and distribute a comprehensive, campus-wide patch management standard by November 30, 2010.
- c. The campus information security standards will require approval for administrative access to servers by November 30, 2010.
- d. The campus will define security responsibilities for designated IT personnel to update their job descriptions by November 30, 2010.

E-MAIL SYSTEMS

The campus had not developed policies and procedures for the multiple e-mail systems used by decentralized departments.

The director of technology services, administration and finance/information security officer stated that the existence of multiple e-mail systems was primarily due to departmental and college desires for specific calendaring functionality.

The lack of policies and procedures for the administration of e-mail systems increases the risk that the various IT business units may not be performing leading security practices over common e-mail exploits and makes it more difficult to ensure emergency notification lists are current. Should the

campus become involved in legal discovery proceedings, it may also risk being unable to recover e-mails because they have not been appropriately retained.

Recommendation 8

We recommend that the campus develop and implement policies and procedures to address the administration of the e-mail systems used by decentralized departments.

Campus Response

We concur. The campus will develop and implement policies and procedures to address the administration of the e-mail systems used by decentralized departments by October 8, 2010.

TECHNICAL VULNERABILITIES

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

Our external testing of selected servers disclosed 25 vulnerabilities on a variety of servers. We provided the specific details of these vulnerabilities to the campus.

Also, the central ITS department did not coordinate the deployment of servers in the decentralized computing environment, nor did it provide professional standards and guidance related to such deployments. The decentralized servers were not routinely patched, and there were no baseline security standards for server or application security.

The director of technology services, administration and finance/information security officer stated that the lack of centralized IT oversight and direction had permitted the majority of these vulnerabilities to propagate in the decentralized computing environments.

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 9

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that remediates security vulnerabilities prior to deployment.

- c. Ensure that the security baseline standard is used by all the ancillary IT units.

Campus Response

We concur. The campus will provide a response for all of the technical vulnerabilities that were identified and presented in detail by November 30, 2010. Most of the vulnerability repairs have been completed.

- a. The campus will develop and distribute a comprehensive, campus-wide patch management standard by November 30, 2010.
- b. The campus will formalize a security baseline standard that remediates security vulnerabilities prior to deployment by November 30, 2010.
- c. The campus will ensure that the security baseline standard is used by all the ancillary IT units by November 30, 2010.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

The web application development and change management practices required improvement.

Specifically, we noted that:

- ▶ Change control practices had not been formalized to provide guidelines and documentation requirements for change request approvals, testing of programming code, user acceptance testing, management of source code, and the migration of changes to production.
- ▶ Application security acceptance was not coordinated with the information security officer.
- ▶ Web security reviews were not performed to identify potential web application code vulnerabilities before being moved to production.
- ▶ Some developers had unlimited access to the source code in production environments and moved their own program changes to production.
- ▶ There was no source code version control process to ensure the integrity of source code in some environments.
- ▶ Production environments were not always separated from test environments.

The director of technology services, administration and finance/information security officer stated that central ITS department staff and decentralized department staff had various development practices but had not formalized the change management process and security requirements for web application development.

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

Recommendation 10

We recommend that the campus:

- a. Require documented approval of all web application projects and change requests prior to development and placement into production.
- b. Develop a security standard that requires the review of applications for security vulnerabilities prior to deployment.
- c. Develop formal documentation criteria for testing procedures for all application development departments.
- d. Develop formal user acceptance testing procedures for all departments.
- e. Limit developers' ability to move web applications into production, or create procedures so that changes to production are monitored by management.
- f. Implement version control and a check-out process to track changes and ensure the integrity of source code for all departments.
- g. Ensure all departments follow formal change control procedures.
- h. Create and test environment for all departments to ensure that changes are adequately tested prior to being moved to production.

Campus Response

We concur. The campus will develop and formalize standards that address the above recommendations for web application development and change management practices by October 21, 2010.

SYSTEMS SECURITY AND MONITORING

CONTROL OVER USER ACCESS

Administration and management of user access profiles required improvement.

Our review of several non-PeopleSoft systems that contained confidential data disclosed that:

- ▶ Data custodians had not performed periodic user access reviews for validating system access and/or permissions.
- ▶ Formal approval for new users with access to sensitive information was not consistently obtained.
- ▶ Transferred employees' prior system and network access to information assets had not been consistently removed.
- ▶ Documentation evidencing the timely removal of separated employees' access to the systems and network could not be provided.

The director of technology services, administration and finance/information security officer stated that the central ITS department and various campus colleges/departments had not established a formalized process for either periodic user access reviews or user provisioning for new users, transfers, and separations.

Failure to periodically review user access increases the risk of inappropriate access. Failure to properly administer provisioning of user accounts increases the risk of inappropriate access.

Recommendation 11

We recommend that the campus:

- a. Conduct and document periodic reviews of user access to systems containing protected data, at least annually.
- b. Create a formal process for approving and removing user accounts.

Campus Response

We concur.

- a. The campus will develop and distribute standards requiring information authorities to conduct periodic reviews of user access to systems containing protected data at least annually by November 30, 2010.

- b. The campus will create formal processes for approving and removing user accounts by November 30, 2010.

PASSWORD STANDARDS

Password standards for centralized and decentralized IT environments required improvement.

We found that:

- ▶ The campus password policy did not require the following password standards: encryption, number of failed access attempts, account lockout duration, and session timeout.
- ▶ Stricter password complexity standards had not been defined for privileged user and administrator accounts.
- ▶ The campus' password standards had not been enforced upon various departments and colleges.

The director of technology services, administration and finance/information security officer stated that various campus-wide IT staff had established their own password management practices, but should have complied with the campus administrative password policy and standards.

The lack of a consistent password policy increases the risk that password parameters within campus systems will be insufficient, which could increase the risk of unauthorized access to network resources and confidential information.

Recommendation 12

We recommend the campus establish and implement a stricter password policy and ensure that all departments comply with that policy.

Campus Response

We concur. The campus will develop a stricter password policy and require department compliance by October 8, 2010.

NETWORK ARCHITECTURE

Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources.

Normally, Internet-accessible devices are segmented into a demilitarized zone so that if these devices are compromised, they are separated from other internal network resources.

The director of communications and computing services stated that the central ITS and academic affairs network segments had been firewalled-off and segregated from the campus internal network.

The remaining network segments within the internal campus network had not been segregated due to resource constraints.

Inadequate segmentation of publicly accessible devices from internal resources increases the risk that compromised devices could be used to pivot to other network targets and launch attacks against internal resources.

Recommendation 13

We recommend that the campus review its current network topology and determine the most logical way to separate Internet-accessible devices from other devices within the internal network.

Campus Response

We concur. The campus will determine an appropriate method to protect confidential information and ensure data integrity and access by October 8, 2010.

BASELINE SECURITY STANDARDS

Baseline security standards for the administration of campus-wide servers and desktops had not been developed.

The director of technology services, administration and finance/information security officer stated that the campus had implemented campus administrative information security policies but had not developed baseline security standards due to competing priorities such as the draft CSU systemwide information security policies and standards project.

The lack of baseline security standards increases the risk of misconfigured systems that could leave the campus vulnerable to malicious attacks.

Recommendation 14

We recommend that the campus develop campus-wide baseline security standards for the administration of servers and desktop systems.

Campus Response

We concur. The campus will develop baseline security standards for administering servers and desktop systems by November 30, 2010.

VULNERABILITY MANAGEMENT

The campus lacked a consistent process for detecting vulnerabilities related to the security of servers and desktops connected to the campus network.

Although the campus performed scans on an as-needed basis, it did not have a consistent standard for monitoring, detecting, and remediating campus-wide vulnerabilities and exploits to ensure compliance with campus-wide policies.

The director of communications and computing services stated that the campus does not have a vulnerability management program and intrusion detection system due to lack of resources and competing priorities.

Failure to address identified vulnerabilities may compromise network resources and lead to the loss of protected confidential information.

Recommendation 15

We recommend that the campus develop a consistent process to detect vulnerabilities on all servers and desktops connected to the campus network.

Campus Response

We concur. The campus will develop a consistent process to detect vulnerabilities for servers and desktops connected to the campus network by October 21, 2010.

REVIEW OF SECURITY EVENT LOGS

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

The director of technology services, administration and finance/information security officer stated that campus-wide IT personnel had various security log management practices but had not documented them consistently.

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 16

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. This process could

include the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating processes.

- b. Consider the implementation of security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

Campus Response

We concur.

- a. The campus will develop formal processes to review and analyze security event logs to identify network vulnerabilities and breaches of campus systems by November 30, 2010.
- b. The campus will evaluate the implementation of tools for centralized security monitoring that provide trend analysis, logging, and automated notification by November 30, 2010.

NETWORK ACCESS

The campus did not adequately secure the campus local-area network (LAN) and lacked a formal process to identify all types of servers on the campus network.

We found that:

- ▶ The campus did not control computer access to the campus LAN. The campus permitted colleges and departments to allow automatic wired access via any operable Ethernet jack to all computers without requiring authentication or confirmation of adequate security updates.
- ▶ The campus practices of assigning static Internet Protocol (IP) requests did not provide a means for the campus to assess and document the security and appropriateness of the device assigned to the IP address.

The director of communications and computing services stated that different decentralized LAN coordinators have different practices for managing network access and for the network management of static IP addresses.

Inadequate control over access to the campus network increases the risk of loss and inappropriate use of state resources and increases campus exposure to information security breaches.

Recommendation 17

We recommend that the campus:

- a. Implement a formal process to require campus users who acquire network access to provide verification of adequate patch management, antivirus updates, and compliance with campus security requirements.

- b. Implement a process to identify all campus-owned IT assets connected to the network (including hardware, software, operating system versions, etc.), and monitor them for adequate security.

Campus Response

We concur.

- a. The campus will develop a formal process to verify campus users who acquire network access to be in compliance with campus security requirements by October 8, 2010.
- b. The campus will develop a process to verify campus-owned IT assets connected to the network comply with security requirements by October 8, 2010.

THREAT MANAGEMENT

The campus did not have an intrusion detection system to monitor and report security threats.

The director of communications and computing services stated that the campus responded to network intrusion incidents when it identified them. The campus had not implemented a network detection system due to resource constraints.

The lack of an intrusion detection system for monitoring and responding to security incidents increases the risk of loss and inappropriate use of state resources and increases campus exposure to information security breaches.

Recommendation 18

We recommend that the campus implement an intrusion detection system to monitor and report potential security threats and that it assess all campus modem use for adequate security.

Campus Response

We concur. The campus will develop detection processes to monitor and report potential intrusion security threats and assess all campus modem use for adequate security by November 30, 2010.

CONFIGURATION CHANGES

The campus lacked policies and procedures that defined a formal, periodic review of configuration changes for firewalls, switches, routers and operating systems.

Periodic reviews of these systems and devices were occurring informally at regular intervals as part of the network operational responsibilities; however, this informal process was not adequate to ensure that these network devices adhered to the latest configuration standards and updates.

The director of communications and computing services stated that a lack of resources did not allow for a formal, periodic review of device configurations.

The lack of formal policies and procedures for reviewing system and device configuration changes decreases accountability for changes made to critical assets. This also increases the risk of inconsistent and deprecated configuration standards, which may permit malicious activity to go undetected.

Recommendation 19

We recommend that the campus:

- a. Develop policies and procedures that establish a formal review of device configurations in order to assist management with determining accountability for potentially misconfigured network devices and with assigning responsibility for identifying and remediating configuration problems.
- b. Incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance with configuration reviews.

Campus Response

We concur.

- a. The campus will develop policies and procedures that establish a formal review of firewall, switch, and router device configurations by October 8, 2010.
- b. The campus will develop a formal sign-off process to ensure compliance with configuration reviews by October 8, 2010.

GRANTING ADMINISTRATIVE ACCESS

The campus lacked a formal process for granting and managing privileged system-level access to accounts on all servers.

The director of technology services, administration and finance/information security officer stated that the campus-wide IT departments and colleges had not formalized the process for granting privileged access.

The lack of a formal process for granting and managing privileged system-level access may lead to inadequate segregation of duties, the granting of accounts not based on the principle of least privilege, and/or unauthorized access.

Recommendation 20

We recommend that the campus establish a formal process for granting and managing privileged system-level access to accounts and that it develop a method to track, review, and periodically audit this type of access.

Campus Response

We concur. The campus will establish a formal process for granting and managing privileged system-level access to server accounts and develop a method to track, review, and audit this type of access by November 30, 2010.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

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

Our review of the border firewall and selected routing and switching devices disclosed that:

- ▶ There were no management host addresses configured for the border firewall.
- ▶ There was no access control list enabled to restrict administrative access to a campus router.
- ▶ Four devices were configured with Simple Network Management Protocol (SNMP). SNMP is unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ Three devices were enabled with Telecommunication Network (Telnet). Because Telnet transfers user logins, passwords, and commands across the network in clear text, this could allow a remote attacker to obtain confidential authentication tokens, which could enable remote access to the devices.

The director of communications and computing services stated that the lack of resources did not allow for a formal, periodic review of device configurations.

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 21

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

In addition, we recommend that the campus:

- a. Create a formal security standard and require the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the network environment to identify potential or known vulnerabilities.

Campus Response

We concur.

- a. The campus will create a formal security standard and require the review of network devices for security vulnerabilities prior to deployment by November 30, 2010.
- b. The campus will develop a comprehensive campus-wide patch management standard for network firewall, routing, and switch devices by November 30, 2010.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

The campus had not completed a campus-wide assessment to identify sensitive data on all servers and workstations, and it did not have a formal process to identify, approve, or review access to confidential information owned and managed by campus ancillary sites. The campus did not have an official approved data classification and handling policy.

The director of technology services, administration and finance/information security officer stated that the campus had not completed its confidential data inventory by the start of the audit.

Inadequate accountability for protected and/or personal confidential information increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 22

We recommend that the campus:

- a. Complete a campus-wide assessment to identify sensitive data on all servers and workstations.
- b. Develop a formal process to identify, approve, or review access to confidential information owned and managed by campus ancillary sites.

Campus Response

We concur.

- a. The campus will complete a campus-wide assessment to identify sensitive data on servers and workstations by October 8, 2010.
- b. The campus will develop a formal process to identify, approve, or review access to confidential information owned and managed by campus ancillary IT units by October 8, 2010.

SYSTEM BACKUP ENCRYPTION

Backup copies of decentralized department systems with protected data were not encrypted.

We noted that:

- ▶ Campus-wide security procedures had not been developed in order to determine encryption requirements for computers, system backups, external hard drives, and universal serial bus (USB) flash drives that store protected data.
- ▶ Laptops, external hard drives, and USB flash drives containing protected data were not encrypted.

The director of technology services, administration and finance/information security officer stated that the campus had not conducted a risk assessment to evaluate the use of encryption as a safeguard for protected data.

Inadequate security related to protected data increases the likelihood of inappropriate access.

Recommendation 23

We recommend that the campus:

- a. Formalize security procedures and conduct a risk assessment to determine encryption requirements for system backup tapes, laptops, external hard drives, and USB flash drives that store protected data.
- b. Encrypt any system backups, laptops, external hard drives, and USB flash drives that contain protected data when stored at off-site locations.

Campus Response

We concur.

- a. The campus will formalize security procedures and conduct a risk assessment to determine encryption requirements for system backup tapes, laptops, external hard drives, and USB flash drives that store protected data by October 21, 2010.
- b. The campus will adopt standards and practices to encrypt any devices that contain protected data when stored at off-site locations by October 21, 2010.

INCIDENT RESPONSE MANAGEMENT

The current incident response process required improvement.

We found that:

- ▶ The campus had no formal process to identify types, frequency, and cost of information security incidents.
- ▶ Security incidents were not formally reported to executive management.

The director of technology services, administration and finance/information security officer stated that although the campus tracked security incidents through a confidential ticketing system, it did not have a process to formally escalate this information to management. She further stated that the campus provided incident reports as requested and provided web access to all California Senate Bill 1386 incidents.

The lack of a formal monitoring and reporting process for security incidents increases the risk of loss and inappropriate use of state resources, and increases the campus' exposure to information security breaches.

Recommendation 24

We recommend that the campus:

- a. Develop a process to identify the types, frequency, and costs of security incidents so that it can monitor trends and risks on campus.
- b. Ensure that security incidents are reported to executive management.

Campus Response

We concur. The campus will develop a process to identify the types, frequency, and costs of security incidents to monitor trends and risks and ensure they are reported to executive management by October 8, 2010.

DISPOSITION OF PROTECTED DATA

The campus' process for ensuring that all sensitive information on computers and laptops was properly deleted prior to the computers' redeployment required improvement.

We noted that the campus' asset management system did not track all IT resources worth less than \$500 that could have contained sensitive information and should have been subject to the deletion of protected data.

The director of technology services, administration and finance/information security officer stated that an outdated property survey form to verify the deletion of protected data was submitted by the campus department to the campus property office. The director of fiscal services stated that the campus property procedures were based on the value of assets, not on their ability to store data or their potential for security risk.

Inadequate control over equipment assets, especially those containing personal confidential information, increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 25

We recommend that the campus:

- a. Develop a process for redeploying computers to ensure that hard-drive wiping is performed and documented.
- b. Update its property procedures to include the tracking of all equipment that could contain protected data.

Campus Response

We concur.

- a. The campus will develop a process for redeploying computers to ensure that hard-drive wiping is performed and documented by September 10, 2010.
- b. The campus will update its property procedures to include tracking of all equipment that could contain protected data by October 8, 2010.

LOST/STOLEN COMPUTERS

The campus' process to report and investigate lost or stolen equipment that might contain protected data required improvement.

We found that:

- ▶ Lost or stolen equipment was not consistently reported to the information security office.
- ▶ There was no formal process to track the disposition of lost or stolen equipment.
- ▶ The owner of lost or stolen equipment was not required to certify that protected data had not been compromised. Such certification should include definitions and specifics of any protected data that might have been accessed inappropriately.
- ▶ Owners of lost or stolen computers did not consistently complete property survey forms.

The director of technology services, administration and finance/information security officer stated that the campus had property procedures that require departments to notify the information security officer if lost or stolen computers contain confidential information, but the departments might not have complied with the procedures.

Inadequate procedures for the reporting and investigation of lost or stolen equipment, which might contain protected data, increases the risk that information security breaches could go unreported, resulting in significant financial penalty and damage to the campus' reputation.

Recommendation 26

We recommend that the campus:

- a. Ensure that the loss or theft of equipment is consistently reported to the information security office.
- b. Establish a formal process to track the disposition of lost or stolen equipment.
- c. Require the owners of lost or stolen equipment to certify that no protected data has been compromised.
- d. Establish a process to ensure that all property survey forms are completed for lost or stolen computers.

Campus Response

We concur. The campus will implement the above recommendations for lost or stolen computers by October 8, 2010.

USE OF EMPLOYEE-OWNED COMPUTERS

The campus did not enforce antivirus or patch management solutions for employee-owned computers that were used for business and that accessed the campus network.

The director of technology services, administration and finance/information security officer stated that the campus had not developed practices and procedures to ensure non-state-owned computers were secure and virus-free when connected to the campus network.

Failure to prohibit or restrict storage of protected data on employees' personal computers increases the risk that sensitive information could be inadequately secured.

Recommendation 27

We recommend that the campus develop a written policy restricting the storage of protected data on employee-owned computers and that it implement procedures to determine that such computers used for university business are routinely patched and protected from viruses.

Campus Response

We concur. The campus has completed development of a policy restricting the storage of protected data on employee-owned computers. The campus will develop and distribute a comprehensive, campus-wide patch management standard by November 30, 2010.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Warren J. Baker	President
Sharon Anderson	Director, Administrative Computing Services
Richard Asplund	Information Technology Consultant, College of Business
Miles Clark	Information Technology Consultant, College of Engineering
Anthony Colvard	Information Technology Coordinator, Associated Students Incorporated
Ken Delmese	Property Clerk II
Tom Dresel	Information Technology Consultant, College of Liberal Arts
James Feld	Network Analyst
Brent Goodman	Director, Institutional Planning and Analysis
Michael Green	Analyst/Programmer
Joyce Haratani	Associate Director, Human Resource Services
Timothy Kearns	Vice Provost Information Technology/Chief Information Officer
Lorlie Leetham	Director, Fiscal Services
Dee Louie	Accountant II
Johanna Madjedi	Director, Communications and Computing Services
Dan Malone	Analyst/Programmer
David Mason	Network Analyst, Student Academic Affairs
Ryan Matteson	Analyst/Programmer
Fred Mills	Police Dispatcher
Jeff Nadel	Network Analyst, College of Engineering
Greg Porter	Operating System Analyst, Department of Computer Science
Rick Ramirez	Associate Vice President Finance
Tom Randall	Information Technology Consultant, College of Science and Mathematics
Linda Sandy	Director, Information Services Infrastructure
Tony Sawa	Equipment Systems Specialist
Doug Scheel	Network Analyst
Craig Schultz	Director, User Support Services
Mary Shaffer	Information Technology Policy Assurance Officer
Byron Smith	Operating System Analyst, College of Engineering
Eumi Sprague	Information Technology Manager, Cal Poly Corporation
Brenda Tesch	Buyer III Lead
Kinsley Thomas Wong	Information Technology Consultant, University Housing
Terry Vahey	Director of Technology Services, Administration and Finance/ Information Security Officer
Debra Valencia-Laver	Associate Dean, College of Liberal Arts
Rich Walls	Operating System Analyst
Patty Warnick-Wait	Administrative Analyst
Troy Weipert	Support Coordinator, Administration and Finance Division Technology Services



California Polytechnic State University
San Luis Obispo, CA 93407 - 0100

Office of the Vice President
Administration and Finance
(805) 756-2171 • Fax (805) 767-7560

RECEIVED
UNIVERSITY AUDITOR

MAY 28 2010

THE CALIFORNIA STATE
UNIVERSITY

27 May 2010

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

Subject: Campus Responses to Recommendations of Audit Report Number 09-40,
Information Security at California Polytechnic State University, San Luis Obispo

Dear Larry:

Enclosed in reply to your 29 April 2010 letter to President Baker, are Cal Poly's responses to the Information Security audit report (Audit Report No. 09-40). The responses are submitted to you for review and for acceptance by the Chancellor. The responses include a corrective action plan and time frame for completion.

Please direct questions to Terry Vahey, Information Security Officer, at 805-756-7667 (tvahey@calpoly.edu).

Sincerely,

Lawrence Kelley
Vice President for Administration & Finance

cc: W. Baker, T. Vahey, R. Ramirez

INFORMATION SECURITY

CALIFORNIA POLYTECHNIC STATE UNIVERSITY, SAN LUIS OBISPO

Audit Report 09-40

SECURITY GOVERNANCE

INFORMATION SECURITY POLICY

Recommendation 1

We recommend that the campus update its information security policies to address the changing campus IT environments(s) and recent statutory compliance requirements.

Campus Response

We concur. The campus will update its information security policies by 8 October, 2010.

RECORD RETENTION

Recommendation 2

We recommend that the campus:

- a. Complete a record retention action plan and corresponding procedures that ensure its appropriate and timely disposal of records/information in accordance with campus time frames.
- b. Develop and document an e-mail retention policy.

Campus Response

We concur.

- a. The campus will prepare a record retention action plan to ensure its appropriate and timely disposal of records/information in accordance with campus time frames by 8 October, 2010.
- b. The campus will develop and document an e-mail retention policy by 8 October, 2010.

INFORMATION SECURITY

CALIFORNIA POLYTECHNIC STATE UNIVERSITY, SAN LUIS OBISPO

Audit Report 09-40

SECURITY GOVERNANCE

INFORMATION SECURITY POLICY

Recommendation 1

We recommend that the campus update its information security policies to address the changing campus IT environments(s) and recent statutory compliance requirements.

Campus Response

We concur. The campus will update its information security policies by 8 October, 2010.

RECORD RETENTION

Recommendation 2

We recommend that the campus:

- a. Complete a record retention action plan and corresponding procedures that ensure its appropriate and timely disposal of records/information in accordance with campus time frames.
- b. Develop and document an e-mail retention policy.

Campus Response

We concur.

- a. The campus will prepare a record retention action plan to ensure its appropriate and timely disposal of records/information in accordance with campus time frames by 8 October, 2010.
- b. The campus will develop and document an e-mail retention policy by 8 October, 2010.

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 3

We recommend that the campus develop a security awareness training policy and ensure that all employees with access to campus computing resources complete the training.

Campus Response

We concur. The campus will develop a security awareness training program to ensure that all employees with access to campus computing resources complete the training by 8 October, 2010

INFORMATION SECURITY PLAN

Recommendation 4

We recommend that the campus:

- a. Conduct a formal information security risk assessment.
- b. Update the plan to prioritize all information security risks and establish specific timelines for addressing the risks.

Campus Response

We concur. The campus will update its information security risk assessment with updated risks by 8 October, 2010. The campus has completed update of the plan with assigned priorities and timelines for addressing the risks.

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 5

We recommend that the campus:

- a. Provide sufficient management oversight to ensure that security responsibilities are being addressed by the departmental and college information security designees.
- b. Formally define and communicate the information security officer's roles, responsibilities, and authority.
- c. Formalize position/job descriptions to include security responsibilities for designated information technology personnel.

Campus Response

We concur.

- a. The campus will develop a process to monitor departmental and college information security designee's technology environments annually by 21 October, 2010.
- b. The campus will update and communicate the information security officer's roles, responsibilities and authorities in the updated information security program by 21 October, 2010.
- c. The campus will define security responsibilities for designated information technology personnel to update their job descriptions by 21 October, 2010.

INFORMATION SECURITY MANAGEMENT

Recommendation 6

We recommend that the campus:

- a. Develop a process to track and report on the various decentralized computing environments' ongoing compliance with campus information security policies and procedures.
- b. Ensure that relevant campus and college IT staff are adequately trained on their newly defined security responsibilities and procedures.

Campus Response

We concur.

- a. The campus will develop a process to monitor departmental and college information security designee's technology environments annually by 21 October, 2010.
- b. The campus will implement a training plan for campus and IT staff on information security policies, standards and guidelines by 21 October, 2010.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Recommendation 7

We recommend that the campus:

- a. Formally communicate campus-wide information security policies and procedures and enforce compliance in decentralized computing environments.

- b. Ensure that the departments' patch management processes are sufficient to guarantee that the most current software patches are installed in a timely manner.
- c. Eliminate administrative access to computers unless specifically approved.
- d. Ensure that decentralized IT professionals in the colleges and departments have appropriate authority and oversight over information security practices in their computing environments.

Campus Response

We concur.

- a. The campus will formally communicate its information security policies, standards and guidelines to the campus IT staff by 30 November, 2010. The campus will develop a process to monitor and enforce compliance in the decentralized computing environments by 30 November, 2010.
- b. The campus will develop and distribute a comprehensive, campus-wide patch management standard by 30 November, 2010.
- c. The campus information security standards will require approval for administrative access to servers by 30 November, 2010.
- d. The campus will define security responsibilities for designated information technology personnel to update their job descriptions by 30 November, 2010.

E-MAIL SYSTEMS

Recommendation 8

We recommend that the campus develop and implement policies and procedures to address the administration of the e-mail systems used by decentralized departments.

Campus Response

We concur. The campus will develop and implement policies and procedures to address the administration of the e-mail systems used by decentralized departments by 8 October, 2010.

TECHNICAL VULNERABILITIES

Recommendation 9

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.

- b. Formalize a security baseline standard that remediates security vulnerabilities prior to deployment.
- c. Ensure that the security baseline standard is used by all the ancillary IT units.

Campus Response

We concur. The campus will provide a response for all of the technical vulnerabilities that were identified and presented in detail by 30 November, 2010. Most of the vulnerability repairs have been completed.

- a. The campus will develop and distribute a comprehensive, campus-wide patch management standard by 30 November, 2010.
- b. The campus will formalize a security baseline standard that remediates security vulnerabilities prior to deployment by 30 November, 2010.
- c. The campus will ensure that the security baseline standard is used by all the ancillary IT units by 30 November, 2010.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Recommendation 10

We recommend that the campus:

- a. Require documented approval of all web application projects and change requests prior to development and placement into production.
- b. Develop a security standard that requires the review of applications for security vulnerabilities prior to deployment.
- c. Develop formal documentation criteria for testing procedures for all application development departments.
- d. Develop formal user acceptance testing procedures for all departments.
- e. Limit developers' ability to move web applications into production, or create procedures so that changes to production are monitored by management.
- f. Implement version control and a check-out process to track changes and ensure the integrity of source code for all departments.
- g. Ensure all departments follow formal change control procedures.
- h. Create and test environment for all departments to ensure that changes are adequately tested prior to being moved to production.

Campus Response

We concur. The campus will develop and formalize standards that address the above recommendations for Web application development and change management practices by 21 October, 2010.

SYSTEMS SECURITY AND MONITORING

CONTROL OVER USER ACCESS

Recommendation 11

We recommend that the campus:

- a. Conduct and document periodic reviews of user access to systems containing protected data, at least annually.
- b. Create a formal process for approving and removing user accounts.

Campus Response

We concur.

- a. The campus will develop and distribute standards requiring information authorities to conduct periodic reviews of user access to systems containing protected data at least annually by 30 November, 2010.
- b. The campus will create formal processes for approving and removing user accounts by 30 November, 2010.

PASSWORD STANDARDS

Recommendation 12

We recommend the campus establish and implement a stricter password policy and ensure that all departments comply with that policy.

Campus Response

We concur. The campus will develop a stricter password policy and require department compliance by 8 October, 2010.

NETWORK ARCHITECTURE

Recommendation 13

We recommend that the campus review its current network topology and determine the most logical way to separate Internet-accessible devices from other devices within the internal network.

Campus Response

We concur. The campus will determine an appropriate method to protect confidential information and ensure data integrity and access by 8 October, 2010.

BASELINE SECURITY STANDARDS

Recommendation 14

We recommend that the campus develop campus-wide baseline security standards for the administration of servers and desktop systems.

Campus Response

We concur. The campus will develop baseline security standards for administering servers and desktop systems by 30 November, 2010.

VULNERABILITY MANAGEMENT

Recommendation 15

We recommend that the campus develop a consistent process to detect vulnerabilities on all servers and desktops connected to the campus network.

Campus Response

We concur. The campus will develop a consistent process to detect vulnerabilities for servers and desktops connected to the campus network by 21 October, 2010.

REVIEW OF SECURITY EVENT LOGS

Recommendation 16

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. This process could include the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating processes.

- b. Consider the implementation of security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

Campus Response

We concur.

- a. The campus will develop formal processes to review and analyze security event logs to identify network vulnerabilities and breaches of campus systems by 30 November, 2010.
- b. The campus will evaluate the implementation of tools for centralized security monitoring that provide trend analysis, logging, and automated notification by 30 November, 2010.

NETWORK ACCESS

Recommendation 17

We recommend that the campus:

- a. Implement a formal process to require campus users who acquire network access to provide verification of adequate patch management, antivirus updates, and compliance with campus security requirements.
- b. Implement a process to identify all campus-owned IT assets connected to the network (including hardware, software, operating system versions, etc.), and monitor them for adequate security.

Campus Response

We concur.

- a. The campus will develop a formal process to verify campus users who acquire network access to be in compliance with campus security requirements by 8 October, 2010.
- b. The campus will develop a process to verify campus-owned IT assets connected to the network comply with security requirements by 8 October, 2010.

THREAT MANAGEMENT

Recommendation 18

We recommend that the campus implement an intrusion detection system to monitor and report potential security threats and that it assess all campus modem use for adequate security.

Campus Response

We concur. The campus will develop detection processes to monitor and report potential intrusion security threats and assess all campus modem use for adequate security by 30 November, 2010.

CONFIGURATION CHANGES

Recommendation 19

We recommend that the campus:

- a. Develop policies and procedures that establish a formal review of device configurations in order to assist management with determining accountability for potentially misconfigured network devices and with assigning responsibility for identifying and remediating configuration problems.
- b. Incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance with configuration reviews.

Campus Response

We concur.

- a. The campus will develop policies and procedures that establish a formal review of firewall, switch, and router device configurations by 8 October, 2010.
- b. The campus will develop a formal sign-off process to ensure compliance with configuration reviews by 8 October, 2010.

GRANTING ADMINISTRATIVE ACCESS

Recommendation 20

We recommend that the campus establish a formal process for granting and managing privileged system-level access to accounts and that it develop a method to track, review, and periodically audit this type of access.

Campus Response

We concur. The campus will establish a formal process for granting and managing privileged system-level access to server accounts and develop a method to track, review and audit this type of access by 30 November, 2010.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 21

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

In addition, we recommend that the campus:

- a. Create a formal security standard and require the review of network devices for security vulnerabilities prior to deployment.

- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the network environment to identify potential or known vulnerabilities.

Campus Response

We concur.

- a. The campus will create a formal security standard and require the review of network devices for security vulnerabilities prior to deployment by 30 November, 2010.
- b. The campus will develop a comprehensive campus-wide patch management standard for network firewall, routing and switch devices by 30 November, 2010.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Recommendation 22

We recommend that the campus:

- a. Complete a campus-wide assessment to identify sensitive data on all servers and workstations.
- b. Develop a formal process to identify, approve, or review access to confidential information owned and managed by campus ancillary sites.

Campus Response

We concur.

- a. The campus will complete a campus-wide assessment to identify sensitive data on servers and workstations by 8 October, 2010.
- b. The campus will develop a formal process to identify, approve or review access to confidential information owned and managed by campus ancillary IT units by 8 October, 2010

SYSTEM BACKUP ENCRYPTION

Recommendation 23

We recommend that the campus:

- a. Formalize security procedures and conduct a risk assessment to determine encryption requirements for system backup tapes, laptops, external hard drives, and USB flash drives that store protected data.

- b. Encrypt any system backups, laptops, external hard drives, and USB flash drives that contain protected data when stored at off-site locations.

Campus Response

We concur.

- a. The campus will formalize security procedures and conduct a risk assessment to determine encryption requirements for system backup tapes, laptops, external hard drives, and USB flash drives that store protected data by 21 October, 2010.
- b. The campus will adopt standards and practices to encrypt any devices that contain protected data when stored at off-site locations, by 21 October, 2010.

INCIDENT RESPONSE MANAGEMENT

Recommendation 24

We recommend that the campus:

- a. Develop a process to identify the types, frequency, and costs of security incidents so that it can monitor trends and risks on campus.
- b. Ensure that security incidents are reported to executive management.

Campus Response

We concur. The campus will develop a process to identify the types, frequency and costs of security incidents to monitor trends and risks and ensure they are reported to executive management campus by 8 October, 2010.

DISPOSITION OF PROTECTED DATA

Recommendation 25

We recommend that the campus:

- a. Develop a process for redeploying computers to ensure that hard-drive wiping is performed and documented.
- b. Update its property procedures to include the tracking of all equipment that could contain protected data.

Campus Response

We concur.

- a. The campus will develop a process for redeploying computers to ensure that hard-drive wiping is performed and documented by 10 September, 2010.
- b. The campus will update its property procedures to include tracking of all equipment that could contain protected data by 8 October, 2010.

LOST/STOLEN COMPUTERS

Recommendation 26

We recommend that the campus:

- a. Ensure that the loss or theft of equipment is consistently reported to the information security office.
- b. Establish a formal process to track the disposition of lost or stolen equipment.
- c. Require the owners of lost or stolen equipment to certify that no protected data has been compromised.
- d. Establish a process to ensure that all property survey forms are completed for lost or stolen computers.

Campus Response

We concur. The campus will implement the above recommendations for lost or stolen computers by 8 October, 2010.

USE OF EMPLOYEE-OWNED COMPUTERS

Recommendation 27

We recommend that the campus develop a written policy restricting the storage of protected data on employee-owned computers and that it implement procedures to determine that such computers used for university business are routinely patched and protected from viruses.

Campus Response

We concur. The campus has completed development of a policy restricting the storage of protected data on employee-owned computers. The campus will develop and distribute a comprehensive, campus-wide patch management standard by 30 November, 2010.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR



BAKERSFIELD

CHANNEL ISLANDS

July 6, 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 09-40 on *Information Security*,
California Polytechnic State University, San Luis Obispo

LONG BEACH

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of July 6, 2010, I accept the response as submitted with the draft final report on *Information Security*, California Polytechnic State University, San Luis Obispo.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS