February 3, 2015

Dr. Horace Mitchell, President
California State University, Bakersfield
9001 Stockdale Highway
Bakersfield, CA 93311

Dear Dr. Mitchell:

Subject: Audit Report 14-52, Information Security, California State University, Bakersfield

We have completed an audit of Information Security as part of our 2014 Audit Plan, and the final report is attached for your reference. The audit was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

I have reviewed the campus response and have concluded that it appropriately addresses our recommendations. The campus response has been incorporated into the final report, which has been posted to the Office of Audit and Advisory Services' website. We will follow-up on the implementation of corrective actions outlined in the response and determine whether additional action is required.

I wish to express my appreciation for the cooperation extended by the campus personnel over the course of this review.

Sincerely,

Larry Mandel
Vice Chancellor and Chief Audit Officer

cc: Timothy P. White, Chancellor
INFORMATION SECURITY
California State University, Bakersfield

Audit Report 14-52
December 4, 2014
EXECUTIVE SUMMARY

OBJECTIVE
The objectives of the audit were 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 the Integrated California State University Administrative Manual (ICSUAM) information security policy, or where appropriate to an industry-accepted standard, and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

CONCLUSION
Based upon the results of the work performed within the scope of the audit, the operational and administrative controls for information security activities as of September 12, 2014, taken as a whole, were not sufficient to meet the objectives of this audit. In general, the audit revealed that the campus information security program requires attention. Specifically, the campus had not established sufficient governance or oversight for the information security function. It is our opinion that the deficiencies in security governance led directly to many of the other issues that were identified. Explicit authority should be communicated campus-wide regarding those systems and processes that were not centrally managed and not directly under the purview of the campus office of information technology (OIT). Additionally, some security projects had been initiated but had not been completely implemented, such as encryption of workstations and routine scanning of key infrastructure servers. According to management, limited staffing and resources adversely impacted the breadth and scope of security initiatives.

Although objectives were not met, the issues identified do not necessarily suggest that a widespread exposure exists to data security. They do, however, indicate that some attention is needed to ensure that the campus information security program operates in conformance with existing policy and to a level necessary to meet management expectations. Most issues listed below represent opportunities to improve the process and methodologies used to administer the information security program at California State University, Bakersfield.

Specific observations, recommendations, and management responses are detailed in the remainder of this report.
OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. GOVERNANCE AND OVERSIGHT

OBSERVATION

The campus had not formally designated an information security officer or specified the respective security responsibilities and authorities on campus, and the information security office had not developed a formal action plan to identify and prioritize information security risks and a corresponding remediation plan.

We found that:

- The office of information technology (OIT) had not received sufficient authority to implement and oversee information security policy and to facilitate information security efforts across the university.

- The roles and responsibilities of the information security officer were not clearly defined, and the position was staffed on a part-time basis.

- The elevation of information security as a recognized critical responsibility of all campus management had not been effectively communicated.

- The information security position/function did not have sufficient authority to effectively implement security initiatives. As a result, projects like full disk encryption were only partially deployed.

The lack of official designation and authority of an information security officer, the lack of documented job responsibilities and authority, and the absence of a comprehensive information security action plan limit the campus’ ability to direct a comprehensive system of information security management.

RECOMMENDATION

We recommend that the campus:

a. Provide the OIT with sufficient authority to implement and oversee information security policy and to facilitate information security efforts across the university.

b. Define the roles and responsibilities of the information security officer.

c. Communicate the elevation of information security as a recognized critical responsibility of all campus management.

d. Provide the information security position/function with sufficient authority to effectively implement security initiatives.
MANAGEMENT RESPONSE

We concur. The campus is currently reviewing the changes to information security and information technology governance structure and additional funding needed to implement identified information security initiatives. The finalized governance structure will be established by June 3, 2015.

Completed by: June 3, 2015

2. CLOUD COMPUTING POLICY

OBSERVATION

The campus did not have a policy that addressed the security of sensitive data stored in the cloud environment.

Inadequate policies regarding storage of sensitive data in a cloud-based computing environment increases the risk of unauthorized exceptions, could compromise compliance with statutory information security requirements, and could prevent the campus from fully understanding the overall effectiveness of existing security provisions related to protected data.

RECOMMENDATION

We recommend that the campus develop and implement a policy addressing the security of sensitive data stored in the cloud environment.

MANAGEMENT RESPONSE

We concur. The campus will develop and implement a policy for the security of sensitive data stored in the cloud environment.

Completed by: June 3, 2015

3. REMOTE ACCESS TO CAMPUS SYSTEMS

OBSERVATION

The campus did not have any methods to protect the logon credentials of users with access to sensitive data when accessed from unsecured remote workstations, such as home or public computers.

Specifically, campus practices did not protect the logon credentials of PeopleSoft users with extensive data rights and privileges when accessing the system from unsecured computers at remote access points.
Remote access from non-secure workstations increases the risk that sensitive information could be compromised.

RECOMMENDATION

We recommend that the campus implement a method to protect the logon credentials of users with access to sensitive data when accessed from unsecured remote workstations, such as home or public computers.

MANAGEMENT RESPONSE

We concur. We will review and evaluate methods to protect the logon credentials of users with access to sensitive data when accessed from unsecured remote workstations, such as home or public computers, and implement them. For access to sensitive data in PeopleSoft, we will review and document available options and implement a solution in collaboration with CMS.

Completed by: June 3, 2015

4. SERVER AND WORKSTATION VULNERABILITY MANAGEMENT

OBSERVATION

The campus did not regularly perform vulnerability scans of all critical servers and lacked a consistent process for detecting vulnerabilities related to the security of servers and desktops connected to the campus network.

We identified numerous vulnerabilities on servers and workstations. In addition, we noted that some servers were running obsolete versions of operating systems that the vendor no longer supported.

Inadequate scanning of all critical systems and addressing of identified vulnerabilities may compromise network resources and lead to the loss of protected confidential information.

RECOMMENDATION

We recommend that the campus:

a. Perform regular scans of all production servers.
b. Develop a consistent process to detect vulnerabilities on all servers and workstations.
c. Remove or update all obsolete and unsupported operating systems from the network.

MANAGEMENT RESPONSE

We concur.
We will perform regular scans of all production servers, develop a consistent process to detect vulnerabilities on all servers and workstations, and remove or update all obsolete and unsupported operating systems from the network.

Completed by: June 3, 2015

5. INTERNET THREAT MANAGEMENT

OBSERVATION

The campus did not have an intrusion detection system device to detect network attacks from the Internet.

CSU policy requires that system administrators scan and remediate vulnerabilities on critical systems or systems that store protected data. According to the network analyst, 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

We recommend that the campus implement an intrusion detection system to monitor and report potential security threats.

MANAGEMENT RESPONSE

We concur. The campus will implement an intrusion detection system.

Completed by: June 3, 2015

6. DESKTOP SOFTWARE MANAGEMENT

OBSERVATION

The campus did not always remove from computers obsolete versions of software and unauthorized software that did not support university business and did not always update browser software.

Inadequate updating of browser software and removal of vulnerable software products and unauthorized software may lead to compromise and potential loss of protected confidential information or inappropriate access to systems.
RECOMMENDATION

We recommend that the campus remove from computers all obsolete versions of software and unauthorized software that does not support university business and update software on all computers.

MANAGEMENT RESPONSE

We concur. The campus will revise its software management process to include removal of obsolete products and unauthorized software that does not support university business, and update software installed on campus-owned computers.

Completed by: June 3, 2015

7. FIREWALL SETTINGS

OBSERVATION

The campus firewall device was not optimally configured to meet the campus’ desired security objectives.

Our technical analysis identified various security deficiencies with the firewall rules that were in place to control network traffic.

An inadequately configured system increases 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

We recommend that the campus review, assess and, if necessary, adjust firewall settings to remediate identified security deficiencies.

MANAGEMENT RESPONSE

We concur. We will adjust firewall settings to remediate security deficiencies.

Completed by: June 3, 2015

8. DESKTOP SECURITY MANAGEMENT

OBSERVATION

The campus did not have a formal policy governing administrative privileges on campus workstations, and existing Windows Active Directory (AD) settings did not always ensure adequate security.
Specifically, we found that the campus allowed users to have administrative access to their workstations, which allowed disabling of some security controls and installation of unauthorized software. The vulnerability assessment performed by audit revealed that 62 percent of the vulnerabilities and compliance issues discovered were the result of administrative access on workstations. In addition, AD group policies for desktops were not set to enforce session time-outs after a prolonged period of inactivity.

Inadequate control over workstation security could inadvertently introduce malware and harmful software to be installed, and failure to set a limited period for session inactivity could expose networked systems and data to unauthorized access.

**RECOMMENDATION**

We recommend that the campus:

a. Eliminate administrative access to workstations unless specifically approved.

b. Review the current enterprise AD and departmental server policy settings and develop a threshold that adequately balances security and business enablement across the enterprise environment.

**MANAGEMENT RESPONSE**

We concur. We will eliminate administrative access not specifically approved. We will review the current enterprise AD and departmental server policy settings and develop a threshold that adequately balances security and business enablement across the enterprise environment.

Completed by: June 3, 2015

9. **WEBSITE MAINTENANCE AND SECURITY**

**OBSERVATION**

The campus did not perform vulnerability scans on websites before the websites were placed into production and regularly thereafter.

The technical analysis performed by audit identified vulnerabilities on the website reviewed.

Failure to scan websites for vulnerabilities could increase the risk of compromise from hackers and could unintentionally expose sensitive campus information.

**RECOMMENDATION**

We recommend that the campus perform vulnerability scans on websites before the websites are placed into production and regularly thereafter.
MANAGEMENT RESPONSE

We concur. The campus will perform vulnerability scans on websites before the websites are placed into production and regularly thereafter.

Completed by: June 3, 2015

10. E-MAIL POLICY

OBSERVATION

Campus policies and procedures addressing e-mail system usage, retention, and disclosure were not documented.

Specifically, the campus did not have policies to:

- Designate that e-mail is owned by the campus and could be part of the official business records of the campus.
- Describe how long the campus should retain deleted e-mail.

The lack of documented e-mail policies increases the risk of unauthorized use of e-mail systems and possible loss of university records.

RECOMMENDATION

We recommend that the campus create an e-mail policy that:

a. Designates that e-mail is owned by the campus and could be part of the official business records of the campus.

b. Describes how long the campus should retain deleted e-mail.

MANAGEMENT RESPONSE

We concur. We will revise our campus e-mail policy to designate that e-mail is owned by the campus and could be part of the official business records of the campus. We will describe how long the campus should retain deleted e-mail.

Completed by: June 3, 2015
GENERAL INFORMATION

BACKGROUND

The CSU Information Security Policy, dated April 19, 2010, states that the Board of Trustees of the CSU is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act. It is the collective responsibility of all users to ensure confidentiality of information that the CSU must protect from unauthorized access; integrity and availability of information stored on or processed by CSU information systems; and compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.

It further states that the CSU Information Security Policy shall apply to the following:

- All campuses.
- Central and departmentally managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

Auxiliaries, external businesses, and organizations that use campus information assets must also operate those assets in conformity with the CSU Information Security Policy.

The CSU Information Security Policy directs the campus president to appoint an information security officer (ISO) and assign responsibility and authority for administering the information security function.

Information security at CSU campuses covers a broad range of sensitive data that requires protection to be in compliance with numerous state and federal regulations. Campuses collect social security numbers for employee personnel and for student financial aid tax reporting, which is regulated by federal and state law. Other forms of data include student grades and academic records that must be protected under federal privacy laws.

In addition, CSU campuses that have student health centers, psychological counseling centers, and pharmacies may also have medical and prescription records that must be protected under federal health privacy laws.

Campus retail operations for bookstores, convenience stores, restaurants and dining, and student activities involve collection and processing of credit card information that is regulated by the banking industry.
At the CSU Bakersfield campus, information security is going through a transition, and currently there is no one designated as the information security officer. Information security activities are administered on a part-time basis, without documented authority or authorization. Information security activities are administered by a security liaison who is several layers down in the overall campus governance structure, and security initiatives and plans are not formally or regularly reported to executive level campus management.

SCOPE

Our audit and evaluation included the audit tests we considered necessary in determining whether operational and administrative controls are in place and operative. The audit focused on procedures in effect from August 11, 2014, through September 12, 2014.

Specifically, we reviewed and tested:

- The activities/measures undertaken to protect the confidentiality, integrity, and access/availability of information.
- Processes for identifying confidential, private, or sensitive information; authorizing access; securing information; detecting security breaches; and evaluating security incident reporting and response.
- 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.
- Encryption of data in storage and transmission.
- Physical and logical security measures for all data repositories.

We also retained outside 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. Specifically, this configuration testing included assessment of the following technologies: selected operating systems, border firewall settings, network traffic analysis, vulnerability scanning, and website vulnerability assessment.

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 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, and our testing approach was designed to provide a view of the security technologies used to protect only key computing resources. In addition, selected emerging technologies were excluded from the scope of the review.
CRITERIA

Our audit was based upon standards as set forth in CSU Board of Trustee policies; Office of the Chancellor policies, letters, and directives; campus procedures; and other sound administrative practices. This audit was conducted in conformance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

This review emphasized, but was not limited to, compliance with:

- ICSUAM §8000, Information Security
- ICSUAM §7000, Identity Management
- Government Code §11549.3
- International Standards Organization 27001, Information Security Management System Standard

AUDIT TEAM

Senior Director: Mike Caldera
Audit Manager: Greg Dove