SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY,
OFFICE OF THE CHANCELLOR

Audit Report 13-36
October 22, 2013

Members, Committee on Audit

Lupe C. Garcia, Chair
Steven M. Glazer, Vice Chair
Rebecca D. Eisen  William Hauck
Hugo Morales

Staff

Vice Chancellor and Chief Audit Officer: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditor: Kim Pham

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
## CONTENTS

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

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

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Sensitive Data Policy .............................................................................................................. 6

Data Classification .................................................................................................................. 7

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

Human Resources ................................................................................................................... 9
  Information Security Awareness Training ............................................................................. 9
  Background Checks .............................................................................................................. 9

Network Security .................................................................................................................. 10
  Intrusion Detection System ................................................................................................. 10
  Review of Security Event Logs .......................................................................................... 11
  Mobile Devices .................................................................................................................. 12

Access Controls .................................................................................................................... 13

Compliance ............................................................................................................................. 14

Encryption .............................................................................................................................. 15

External Parties ..................................................................................................................... 16
APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Management Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

CO       Office of the Chancellor
CSU      California State University
DSS      Data Security Standard
HR       Human Resources
ICSUAM   Integrated California State University Administrative Manual
IDS      Intrusion Detection System
ISM      Information Security Management
ISO      Information Security Officer
PCI      Payment Card Industry
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of Audit and Advisory Services during the last quarter of 2012, the Board of Trustees, at its January 2013 meeting, directed that Sensitive Data Security and Protection be reviewed. The Office of Audit and Advisory Services had previously reviewed sensitive data at six campuses in 2011.

We visited the Office of the Chancellor (CO) from June 17, 2013, through July 12, 2013, and audited the procedures in effect at that time.

In our opinion, due to the effect of the weaknesses described below, the fiscal, operational, and administrative controls for sensitive data as of July 12, 2013, taken as a whole, were not sufficient to meet the objectives stated above and in the “Purpose” section of this report. Areas of major concern include: sensitive data policy, data classification, asset management, human resources, network security, access control, compliance, encryption, and external parties.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our audit did not examine all controls over sensitive data, but was designed to assess management controls, increase awareness of the topic, and assess regulatory compliance for significant sensitive data categories that are prevalent in the California State University (CSU) 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.

SENSITIVE DATA POLICY [6]

The information security program at the Office of the Chancellor (CO) was not sufficient to ensure employee awareness and compliance with relevant laws, regulations, and California State University (CSU) policies.

DATA CLASSIFICATION [7]

The CO did not perform periodic inventory and controls assessments of all protected data maintained in electronic and paper files.

ASSET MANAGEMENT [8]

Electronic data records stored in PeopleSoft were maintained indefinitely, rather than being retained and disposed of according to CSU policy.
HUMAN RESOURCES [9]

The CO did not require all computer information users to complete information security awareness training. In addition, background checks were not performed on all employees hired into positions with access to sensitive data.

NETWORK SECURITY [10]

The CO did not have an intrusion detection system in place to monitor intrusion security events. Additionally, the review of security event logs was inadequate. Also, the CO had not adequately addressed the risk of protected data being stored on unsecured mobile devices.

ACCESS CONTROL [13]

Physical security of sensitive paper documents was inadequate. Specifically, some sensitive paper documents were stored in unsecured boxes located in open working areas and walkways, and the facilities department had access to all file cabinets at the CO, including file cabinets used to store sensitive paper documents.

COMPLIANCE [14]

The CO had not fully addressed Payment Card Industry (PCI) Data Security Standard (DSS) compliance deficiencies. Specifically, the CO had not installed and maintained a firewall configuration to protect cardholder data, protected stored cardholder data, assigned a unique identification to each person with computer access, restricted physical access to cardholder data, tracked and monitored all access to network resources and cardholder data, regularly tested security systems and processes, or maintained a policy that addressed information security for employees and contractors.

ENCRYPTION [15]

The CO did not store protected data maintained on file servers in an encrypted format.

EXTERNAL PARTIES [16]

The service agreement between the CO and a third-party service provider for box office ticket sales did not contain adequate terms for data confidentiality, information security, and system backups. In addition, the agreement had not been reviewed by procurement or the information security management office prior to execution.
INTRODUCTION

BACKGROUND

Integrated California State University Administrative Manual (ICSUAM) §8000.0, *Information Security Policy*, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding the security and protection of sensitive data. It provides direction for managing and protecting the confidentiality, integrity, and availability of California State University (CSU) information assets and defines the organizational scope of information security throughout the system.

The policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

According to ICSUAM §8000.0, it is the collective responsibility of all users to ensure:

- The confidentiality of information that the CSU must protect from unauthorized access.
- The integrity and availability of information stored on or processed by CSU information systems.
- Compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection.

The policy further states that auxiliary organizations, external businesses, and organizations that use campus information assets must also follow the CSU Information Security Policy.

State Administrative Manual §5300 defines information security as the protection of information and information systems and equipment from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code §11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection in the California Office of Information Security.

At the CSU campuses, the information security officer has overall responsibility for the security and protection of sensitive data, which extends to all campus departments, colleges, and auxiliary organizations.
PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of sensitive data; to determine the adequacy of controls over the related processes; and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, oversight committees, executive-level reporting, and documented policies and procedures.

- A management framework is established to initiate and control the implementation of information security within the organization, and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.

- All assets are accounted for and have a nominated owner/custodian who is responsible for achieving and maintaining appropriate protection of organizational assets, and information is appropriately classified to indicate the expected degree of protection.

- Security responsibilities are addressed with employees prior to the start of employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work.

- Responsibilities and procedures for the management of information processing and service delivery are defined, and technical security controls are integrated within systems and networks.

- Access rights to systems, applications, and business processes surrounding sensitive data are controlled by means of user identification and authentication, based on business and security requirements.

- Formal event reporting and escalation procedures are in place for information security events and weaknesses, and communication is consistent and effective, allowing for timely corrective action.

- The information systems’ design, configuration, operation, use, and management are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.

- Contractual language addressing a third party’s responsibility for protecting sensitive data is appropriate.
INTRODUCTION

SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 22 and 23, 2013, meeting of the Committee on Audit, stated that sensitive data security and protection would include review and compliance with Trustee policy, federal and state directives, and campus policies and procedures; procedures for handling confidential information; communication and employee training; encryption; tracking and monitoring of access to sensitive data; and retention practices for key records. If the sensitive data is maintained by a third party, we would review the involvement of campus information security personnel in the decision process; documentation of campus expectations for handling and securing the data; contract language covering security expectations; and monitoring of third-party performance.

Our study and evaluation were conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors and included the audit tests we considered necessary in determining whether fiscal, operational, and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the administrative, compliance, operational, and technical controls over the security and protection of sensitive data. Specifically, we reviewed and tested:

- Information security policies and procedures.
- Information security organizational structure and management framework.
- Information asset management accountability and classification.
- Human resources security responsibilities.
- Administrative and technical security procedures.
- Access and configuration controls over networks, systems, applications, business processes, and data.
- Incident response, escalation, and reporting procedures.
- Compliance with relevant statutory, regulatory, and contractual security requirements.
- Third-party contractual language regarding handling of sensitive data.

Our testing and methodology was designed to provide a managerial level review of key security practices over sensitive data. Our review did not examine all categories of sensitive data; selected emerging technologies were excluded from the scope of the review. Our testing approach was designed to provide a view of the security used to protect only key computing and business processes.
OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

SENSITIVE DATA POLICY

The information security program at the Office of the Chancellor (CO) was not sufficient to ensure employee awareness and compliance with relevant laws, regulations, and California State University (CSU) policies.

We found that:

- The Information Security Management (ISM) website did not include enough information related to CSU information security policies, procedures, and guidelines to provide adequate guidance to employees.

- There was a lack of employee awareness about laws, regulations, and CSU policies related to information security.

Integrated California State University Administrative Manual (ICSUAM) §8035.200, dated April 19, 2010, states that the security awareness program must provide an overview of campus information security policies, and help individuals recognize and appropriately respond to threats to campus information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. The program must promote awareness of CSU and campus information security policies, standards, procedures, and guidelines; potential threats against campus protected data and information assets; appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets; and CSU and campus notification procedures in the event protected data is compromised. After receiving initial security awareness training, employees must receive regular updates in policies, standards, procedures, and guidelines.

The CO information security officer (ISO) stated that finalization of the new information security awareness training took longer than expected and that there had been a lack of effort to promote information security awareness.

Lack of information security awareness for employees with access to computer resources increases the risk of mismanagement of protected data, which increases the entity’s exposure to security breaches and could compromise compliance with statutory information security requirements.

Recommendation 1

We recommend that the CO update the information security program by:

a. Updating the ISM website to include additional information regarding CSU information security policies, procedures, and guidelines.

b. Promoting information security awareness through communications such as CO in the Know.
Management Response

We concur. The CO ISM team will update the ISM website to include information regarding CSU information security policies, procedures, and guidelines. Additionally, the ISM team has opened work orders with CO Communications, which will allow us to include periodic articles and tips in CO in the Know promoting security awareness.

Target completion date: March 2014

DATA CLASSIFICATION

The CO did not perform periodic inventory and controls assessments of all protected data maintained in electronic and paper files.

ICSUAM §8020, Information Security Risk Management, dated April 19, 2010, states that campuses must develop risk management processes that identify, assess, and monitor risks to information assets containing level 1 and level 2 data as defined in the CSU Data Classification Standard. Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts. Risk assessments are part of an ongoing risk management process. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls. Campuses must document the scope and frequency of the assessment, risk assessment methodology, result of the risk assessment, and mitigation strategies designed to address identified risks.

ICSUAM §8065, Information Asset Management, dated April 19, 2010, states that campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

The CO ISO stated that the CO maintained an inventory of applications with protected data; however, a periodic inventory and controls assessment of all protected data, including paper documents and file servers, had not been a part of CO procedures in the past.

Inadequate accountability over information assets, especially those containing critical and/or personal confidential information, increases the risk of loss and inappropriate use of campus resources and exposure to information security breaches.

Recommendation 2

We recommend that the CO perform periodic inventory and controls assessments of all protected data maintained in electronic and paper files.
Management Response

We concur. The CO ISM team will perform periodic inventory and control assessments of all protected data maintained in electronic and paper files. The CO ISM team will deploy a sensitive data management application to inventory electronic data. Additionally, the CO ISM team will meet with departments that use and store paper files containing sensitive data to implement security controls.

Target completion date: April 2014

ASSET MANAGEMENT

Electronic data records stored in PeopleSoft were maintained indefinitely, rather than being retained and disposed of according to CSU policy.

Executive Order 1031, Systemwide Records/Information Retention and Disposition Schedules Implementation, dated February 27, 2008, states that each campus must ensure appropriate and timely disposal of records/information in accordance with retention and disposition schedule time frames. The campus is responsible for instituting a process for reviewing its records/information as listed on the schedules to determine if they should be destroyed or maintained. At a minimum, this review should be conducted once a year. Additionally, each campus must establish procedures regarding the modification of retention and disposition schedules, as needed, to incorporate records unique to each campus. These schedules must be published by the campus, and copies are to be provided to the Office of the Chancellor, upon request.

The CO ISO stated that the disposal of electronic data records in PeopleSoft was not in line with the CSU retention and disposal policy because PeopleSoft did not have the ability to parse out specific line items for removal.

Noncompliance with CSU requirements for the retention and disposal of electronic data records could increase the impact of loss should an information security breach or data theft occur.

Recommendation 3

We recommend that the CO dispose of electronic data records stored in PeopleSoft according to CSU records retention policy.

Management Response

We concur. The CO ISM team will update the CSU records retention policy to reflect the capabilities of data records stored within PeopleSoft.

Target completion date: April 2014
HUMAN RESOURCES

INFORMATION SECURITY AWARENESS TRAINING

The CO did not require all computer users to complete information security awareness training.

ICSUAM §8035.100, Information Security Awareness and Training, dated April 19, 2010, states that each campus must implement a program for providing appropriate information security awareness and training to employees appropriate to their access to campus information assets. The campus information security awareness program must promote campus strategies for protecting information assets containing protected data. All employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training must be provided to individuals whose job functions require specialized skill or knowledge in information security.

The CO ISO stated that completion of the new information security awareness training took longer than expected. He also stated that the ISM office had been waiting to implement the new training before requiring all individuals with access to computer systems to complete the training.

Lack of information security awareness training for employees with access to computer resources increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

Recommendation 4

We recommend that the CO require all computer users to complete information security awareness training.

Management Response

We concur. The CO ISM team will initiate an information security awareness program, which will ensure all CO personnel comply with ICSUAM §8035.

Target completion date: April 2014

BACKGROUND CHECKS

Background checks were not performed on all employees hired into positions with access to sensitive data.

We reviewed 15 employees hired into sensitive positions, and we found that the CO had not conducted a background check on 12 of them.
ICSUAM §8030, Personnel Information Security, dated April 19, 2010, states that campuses must develop procedures to conduct background checks on positions involving access to level one information assets as defined in the CSU Data Classification Standard.

Coded memorandum Human Resources (HR) 2005-10, Background Checks, dated March 1, 2005, states that it is the campus’ responsibility to initiate background checks either itself or by using an outside vendor prior to the hire and transfer, reclassification, promotion, or reassignment of individuals into sensitive positions. Sensitive positions that require a background check may involve, but are not limited to, those that have responsibility for the care, safety, and security of people, including children and minors, or property; direct access to, or control over, cash, checks, credit cards, and/or credit card account information; authority to commit financial resources of the university through contracts greater than $5,000; control over campus business processes, either through functional roles or system security access; access to detailed personally identifiable information about students, faculty, staff or alumni, which might enable identity theft; access to controlled substances; and possession of building master or sub-master keys for building access.

The director of HR services stated that the previous coded memorandum had provided additional clarification for background checks for CSU employees that was not provided for in coded memorandum HR-2005-10, and therefore, HR staff and hiring departments were unclear on what positions were considered sensitive or would have access to sensitive information.

Lack of background checks for personnel hired into sensitive positions increases the risk of potential misuse or inappropriate disclosure of sensitive data.

**Recommendation 5**

We recommend that the CO perform background checks on all employees hired into positions with access to sensitive data.

**Management Response**

We concur. The CO ISM team will work with CO HR to ensure that new employees with access to sensitive data receive background checks.

Target completion date: March 2014

**NETWORK SECURITY**

**INTRUSION DETECTION SYSTEM**

The CO did not have an intrusion detection system (IDS) in place to monitor and respond to potential security threats.


ICSUAM §8045.100, *Information Technology Security*, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

The CO ISO stated that due to changes in threat profile and current signature-based protection schemes, the IDS for the CO and other campuses was given reduced priority.

Lack of an IDS to monitor and respond to potential security incidents increases CO exposure to information security breaches.

**Recommendation 6**

We recommend the CO install an IDS to monitor and respond to potential security threats.

**Management Response**

We concur. The CO ISM team will open a project to scope, select, and develop an implementation plan for an IDS.

Target completion date: April 2014

**REVIEW OF SECURITY EVENT LOGS**

Review of security event logs was inadequate.

We found that although the network team reviewed firewall log information on a bimonthly basis, there was no process in place to periodically review and analyze other security event logs, such as overall system, network, and device logs.

ICSUAM §8045.100, *Information Technology Security*, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

ICSUAM §8045.500, *Information Technology Security*, dated April 19, 2010, states that records created by monitoring controls (e.g. logging) must be protected from unauthorized access and reviewed regularly.

The associate director of network and security services stated that resource constraints limited the amount of time that personnel could spend manually reviewing logs.

Inadequate review of security 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, which could lead to a breach of confidential information.
Recommendation 7

We recommend that the CO establish a process to periodically review and analyze all security event logs, including overall system, network, and device logs.

Management Response

We concur. The CO ISM team will open a project to scope, select, and develop an implementation plan for a Security Incident and Event Management system.

Target completion date: April 2014

MOBILE DEVICES

The CO had not addressed the risk of protected data being stored on unsecured mobile devices.

We found that the CO did not have methods to prevent data from being stored on alternative media devices that were not appropriately secured, such as iPhones and iPads.

ICSUAM §8010, Establishing an Information Security Program, dated April 19, 2010, states in part that the campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The program should, among other things: a) provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted; and b) develop risk management strategies to identify and mitigate threats and vulnerabilities.

ICSUAM §8045.400, Information Technology Security, dated April 19, 2010, states that campuses must develop and implement controls for securing protected data stored on mobile devices. Protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Campuses must use encryption, or equally effective measures, on all mobile devices that store level 1 data as defined in the CSU Data Classification Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by a designated campus official. Other effective measures include physical protection that ensures only authorized access to protected data.

The CO ISO stated that employees are advised against storing protected data on mobile devices and that encryption should be used if an individual must carry protected information on a mobile device.

Inadequate methods to prevent sensitive data from being stored on unprotected devices increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.
Recommendation 8

We recommend that the CO address the risk of protected data being stored on unsecured mobile devices.

Management Response

We concur. The CO ISM team will assess the risk of protected data being stored on unsecured mobile devices and make a recommendation to CO IT.

Target completion date: March 2014

ACCESS CONTROLS

Physical security of sensitive paper documents was inadequate.

Specifically, we found that:

- Some sensitive paper documents were stored in unsecured boxes located in open working areas and walkways.

- The facilities department had access to all file cabinets at the CO, including file cabinets used to store sensitive paper documents.

ICSUAM §8080, Physical Security, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are stored.

ICSUAM §8060, Access Control, dated April 19, 2010, states that access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets that access protected data that are located in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. Campuses must review and document physical access rights to campus limited-access areas annually.

The CO ISO stated that department managers were not following guidelines provided by the CSU and the ISM office. He further stated that the facilities department had been entrusted with a master key to all file cabinets to provide access, if needed.
Inadequate physical security over sensitive paper documents increases the risk of information security breaches and unauthorized access.

**Recommendation 9**

We recommend that the CO:

a. Secure all sensitive paper documents.

b. Restrict access to filing cabinets that house sensitive paper documents to only those with a need to know, or implement mitigating controls to protect sensitive paper documents stored in filing cabinets.

**Management Response**

We concur. The CO ISM team will work with all CO departments that have access to paper documents containing sensitive data to ensure that security protocols are used to secure those documents. Additionally, the CO ISM team will work with all CO departments to implement protocols that restrict access to filing cabinets that house sensitive paper documents.

Target completion date: April 2014

**COMPLIANCE**

The CO had not fully addressed Payment Card Industry (PCI) Data Security Standard (DSS) compliance deficiencies.

We found that several PCI DSS compliance deficiencies that were identified in an assessment at the CO had not been addressed, including:

- Installation and maintenance of a firewall configuration to protect cardholder data.
- Protection of stored cardholder data.
- Assignment of a unique login account to each person with computer access.
- Restriction of physical access to cardholder data.
- Tracking and monitoring of all access to network resources and cardholder data.
- Regular testing of security systems and processes.
- Maintenance of a policy that addresses information security for employees and contractors.

ICSUAM §8045.100, *Information Technology Security*, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.
The PCI DSS is a set of comprehensive requirements for enhancing payment account data security, which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. According to payment brand rules, all merchants and their service providers are required to comply with the PCI DSS in its entirety.

The CO ISO stated that the CO was not compliant with all PCI DSS requirements because a PCI compliance program had just recently been implemented.

Noncompliance with PCI DSS requirements exposes the CO to potential financial penalties and credit card usage restrictions, which could include termination of the entity’s ability to accept credit cards.

**Recommendation 10**

We recommend that the CO fully address all PCI DSS compliance deficiencies.

**Management Response**

The CO ISM team will review the existing assessment and provide a recommendation to the affected business units.

*Target completion date: April 2014*

**ENCRYPTION**

The CO did not store protected data maintained on file servers in an encrypted format.

ICSUAM §8045, *Information Technology Security*, dated April 19, 2010, states that each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

ICSUAM §8065, *Information Asset Management*, dated April 19, 2010, states that campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard and that these assets must be categorized and protected throughout their entire life cycle, from origination to destruction.
The CO ISO stated that application owners are responsible for the security of data at rest, taking into consideration the level of risk and other mitigating controls currently in place, and that existing practices did not include independent review by the ISO.

Lack of encryption for protected data increases the risk of loss or inappropriate use of such data and increases the risk of information security breaches, which could require the campus to notify all affected parties, adversely affecting the campus’ reputation.

**Recommendation 11**

We recommend that the CO store all protected data maintained on file servers in an encrypted format.

**Management Response**

We concur. The CO ISM team will open a project to scope, select, and develop an implementation plan for a system to encrypt data on file servers.

Target completion date: April 2014

**EXTERNAL PARTIES**

The service agreement between the CO and a third-party service provider for box office ticket sales needed improvement.

Specifically, we found that the agreement with the Vendini ticket system:

- Did not contain adequate contractual terms for data confidentiality; information security, such as Vendini’s responsibility for addressing data breaches and securing cardholder data; and system backup responsibilities.

- Was not reviewed by procurement or the ISM office prior to execution.

ICSUAM §8040, *Managing Third Parties*, states that third parties who access CSU information assets must be required to adhere to appropriate CSU and campus information security policies and standards. As appropriate, a risk assessment must be conducted to determine the specific implications and control requirements for the service provided. Additionally, third party service providers must not be granted access to campus level 1 or level 2 information assets as defined in the CSU Data Classification Standard until the access has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.

The CO ISO stated that procurement and the ISM office were not involved in the initial contract process with Vendini because the department that procured the services was unaware that the process for granting access to sensitive company information included obtaining authorization from
procurement and ISM management. He further stated that as a result, procurement and ISM management were unable to ensure adequate terms for data confidentiality, information security, and system backups.

Inadequate service agreements subject the CO to potential liability, increase exposure to security breaches, increase the likelihood of misunderstandings for services provided, and could compromise compliance with statutory information security requirements.

**Recommendation 12**

We recommend that the CO:

a. Amend the cited service agreement with appropriate provisions for data confidentiality, information security, and system backup responsibilities.

b. Obtain procurement and ISM’s review on all agreements with third-party service providers who access, process, or manage sensitive data prior to execution.

**Management Response**

We concur. The CO ISM team is working with procurement to include supplemental provisions to the CO’s general provisions. These supplemental provisions will include responsibilities for data confidentiality, information security, and system backup responsibilities. Additionally, the CO ISM team will work with procurement to ensure that ISM reviews all agreements with third-party service providers who access, process, or manage sensitive data prior to execution.

Target completion date: March 2014
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benjamin F. Quillian</td>
<td>Executive Vice Chancellor and Chief Financial Officer (At time of review)</td>
</tr>
<tr>
<td>Sally Roush</td>
<td>Interim Executive Vice Chancellor for Business and Finance</td>
</tr>
<tr>
<td>Amy Ahearn</td>
<td>Financial Information Systems Administrator</td>
</tr>
<tr>
<td>George Ashkar</td>
<td>Assistant Vice Chancellor/Controller, Financial Services</td>
</tr>
<tr>
<td>Lilian Audet</td>
<td>Assistant Director, Finance</td>
</tr>
<tr>
<td>Sean Berry</td>
<td>Administrative Assistant</td>
</tr>
<tr>
<td>Judy Botelho</td>
<td>Director, Center for Community Engagement</td>
</tr>
<tr>
<td>Renata Bouwmeester</td>
<td>Assistant Director, Academic Services</td>
</tr>
<tr>
<td>Bruce Briggs</td>
<td>Assistant Vice Chancellor, Information Technology Services and Chief Information Officer</td>
</tr>
<tr>
<td>Anne Brown</td>
<td>Director, Foundation Programs and Services</td>
</tr>
<tr>
<td>Chris Canfield</td>
<td>Associate Budget Director</td>
</tr>
<tr>
<td>Lorissa Cheney</td>
<td>Financial Information Systems Specialist</td>
</tr>
<tr>
<td>Jolene Colman</td>
<td>Secretary, International Programs</td>
</tr>
<tr>
<td>Marco Garret</td>
<td>Assistant Director, Access Services</td>
</tr>
<tr>
<td>Ellyce Gordon</td>
<td>Property Clerk</td>
</tr>
<tr>
<td>Gerry Hanley</td>
<td>Senior Director, Academic Technology</td>
</tr>
<tr>
<td>Alexander Harwood</td>
<td>Information Security Officer, Chancellor’s Office</td>
</tr>
<tr>
<td>Kristy Hawman</td>
<td>Director, Human Resources (HR) Services</td>
</tr>
<tr>
<td>Yves Hepperle</td>
<td>Project Development Manager</td>
</tr>
<tr>
<td>Tammy Hines</td>
<td>Senior Manager, Common Management System, HR Systemwide</td>
</tr>
<tr>
<td>Linda Horan</td>
<td>Data Analyst/Learn Media Coordinator</td>
</tr>
<tr>
<td>Edward Hudson</td>
<td>Information Security Director</td>
</tr>
<tr>
<td>Melody Kojima</td>
<td>Assistant Director, Purchasing</td>
</tr>
<tr>
<td>Thoa Le</td>
<td>Director, Chancellor’s Office Budget</td>
</tr>
<tr>
<td>Adam Litman</td>
<td>Director, HR Technical Support Services</td>
</tr>
<tr>
<td>Monica Malhotra</td>
<td>Associate Director, Analytic Studies</td>
</tr>
<tr>
<td>Michael McBride</td>
<td>Director, Application Development</td>
</tr>
<tr>
<td>Dawn McKinley</td>
<td>Senior Manager, Compensation and HR Information Projects</td>
</tr>
<tr>
<td>Ty Melvin</td>
<td>Web Page Coordinator</td>
</tr>
<tr>
<td>Tony Modiri</td>
<td>Operations and Network Administrator</td>
</tr>
<tr>
<td>Ruth Hirai</td>
<td>Labor and Employee Relations Analyst</td>
</tr>
<tr>
<td>Marsha Hirano-Nakanishi</td>
<td>Assistant Vice Chancellor, Academic Research and Resource</td>
</tr>
<tr>
<td>William Perry</td>
<td>Chief Information Management and Security Officer</td>
</tr>
<tr>
<td>Tosha Pham</td>
<td>Applications Support Manager</td>
</tr>
<tr>
<td>Shannon Pringle</td>
<td>Production Manager, Summer Arts Program</td>
</tr>
<tr>
<td>Lori Redfearn</td>
<td>Assistant Vice Chancellor, Advancement Services</td>
</tr>
<tr>
<td>Mike Redmond</td>
<td>Acting Assistant Vice Chancellor, Headquarters Building Security and Strategic Initiatives</td>
</tr>
<tr>
<td>Tom Roberts</td>
<td>Director, Contracts and Procurement</td>
</tr>
<tr>
<td>Dana Ronson</td>
<td>Assistant Director, Student Affairs</td>
</tr>
<tr>
<td>DaMonique Sampson</td>
<td>Common Management System Functional Analyst/Programmer</td>
</tr>
<tr>
<td>Jason Solis</td>
<td>Associate Director, Network and Security Services</td>
</tr>
<tr>
<td>Virginia Soto</td>
<td>Student Funds Coordinator</td>
</tr>
<tr>
<td>Dana Twedell</td>
<td>Manager, Facilities</td>
</tr>
</tbody>
</table>
MEMORANDUM

DATE: January 22, 2014

TO: Larry Mandel
University Auditor

FROM: Sally F. Roush
Interim Vice Chancellor

SUBJECT: Audit Report # 13-36 Sensitive Data and Protection

In response to the "Incomplete Draft" report dated October 22, 2013, we are providing the enclosed management response.

Should you have any questions, please contact us.

SFR:mpr

Attachment

cc: Mark Crase, Interim AVC and CIO, Information Technology Services
William Perry, Chief Information Management and Security Officer
Michael Redmond, Acting Assistant Vice Chancellor, Headquarters Budget, Security, and Strategic Initiatives
SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR
Audit Report 13-36

SENSITIVE DATA POLICY

Recommendation 1

We recommend that the CO update the information security program by:

a. Updating the ISM website to include additional information regarding CSU information security policies, procedures, and guidelines.

b. Promoting information security awareness through communications such as CO in the Know.

Management Response

We concur. The CO Information Security Management team will update the ISM website to include information regarding CSU information security policies, procedures, and guidelines. Additionally, the ISM team has opened work orders with CO Communications, which will allow us to include periodic articles and tips in CO in the Know promoting security awareness.

Target completion date: March 2014

DATA CLASSIFICATION

Recommendation 2

We recommend that the CO perform periodic inventory and controls assessments of all protected data maintained in electronic and paper files.

Management Response

We concur. The CO Information Security Management team will perform periodic inventory and control assessments of all protected data maintained in electronic and paper files. The CO ISM team will deploy a sensitive data management application to inventory electronic data. Additionally, the CO ISM team will meet with departments that use and store paper files containing sensitive data to implement security controls.

Target completion date: April 2014
ASSET MANAGEMENT

Recommendation 3

We recommend that the CO dispose of electronic data records stored in PeopleSoft according to CSU records retention policy.

Management Response

We concur. The CO Information Security Management team will update the CSU records retention policy to reflect the capabilities of data records stored within PeopleSoft.

Target completion date: April 2014

HUMAN RESOURCES

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 4

We recommend that the CO require all computer users to complete information security awareness training.

Management Response

We concur. The CO ISM team will initiate an information security awareness program, which will ensure all CO personnel comply with ICSUAM §8035.

Target completion date: April 2014

BACKGROUND CHECKS

Recommendation 5

We recommend that the CO perform background checks on all employees hired into positions with access to sensitive data.

Management Response

We concur. The CO Information Security Management team will work with CO HR to ensure that new employees with access to sensitive data receive background checks.

Target completion date: March 2014
NETWORK SECURITY

INTRUSION DETECTION SYSTEM

Recommendation 6

We recommend the CO install an IDS to monitor and respond to potential security threats.

Management Response

We concur. The CO Information Security Management team will open a project to scope, select, and develop an implementation plan for an Intrusion Detection System.

Target completion date: April 2014

REVIEW OF SECURITY EVENT LOGS

Recommendation 7

We recommend that the CO establish a process to periodically review and analyze all security event logs, including overall system, network, and device logs.

Management Response

We concur. The CO Information Security Management team will open a project to scope, select, and develop an implementation plan for a Security Incident and Event Management (SIEM) system.

Target completion date: April 2014

MOBILE DEVICES

Recommendation 8

We recommend that the CO address the risk of protected data being stored on unsecured mobile devices.

Management Response

We concur. The CO Information Security Management team will assess the risk of protected data being stored on unsecured mobile devices and make a recommendation to CO IT.

Target completion date: March 2014
ACCESS CONTROLS

Recommendation 9

We recommend that the CO:

a. Secure all sensitive paper documents.

b. Restrict access to filing cabinets that house sensitive paper documents to only those with a need to know, or implement mitigating controls to protect sensitive paper documents stored in filing cabinets.

Management Response

We concur. The CO Information Security Management team will work with all CO departments that have access to paper documents containing sensitive data to ensure that security protocols are used to ensure those documents. Additionally, the CO ISM team will work with all CO departments to implement protocols that restrict access to filing cabinets that house sensitive paper documents.

Target completion date: April 2014

COMPLIANCE

Recommendation 10

We recommend that the CO fully address all PCI DSS compliance deficiencies.

Management Response

The CO Information Security Management team will review the existing assessment and provide a recommendation to the affected business units.

Target completion date: April 2014

ENCRYPTION

Recommendation 11

We recommend that the CO store all protected data maintained on file servers in an encrypted format.

Management Response

We concur. The CO Information Security Management team will open a project to scope, select, and develop an implementation plan for a system to encrypt data on file servers.
Target completion date: April 2014

EXTERNAL PARTIES

Recommendation 12

We recommend that the CO:

a. Amend the cited service agreement with appropriate provisions for data confidentiality, information security, and system backup responsibilities.

b. Obtain procurement and ISM’s review on all agreements with third-party service providers who access, process, or manage sensitive data prior to execution.

Management Response

We concur. The CO Information Security Management team is working with procurement to include supplemental provisions to the CO’s general provisions. These supplemental provisions will include responsibilities for data confidentiality, information security, and system backup responsibilities. Additionally, the CO Information Security Management team will work with procurement to ensure that ISM reviews all agreement with third-party service providers who access, process, or manage sensitive data prior to execution.

Target completion date: March 2014
March 4, 2014

MEMORANDUM

TO: Mr. Larry Mandel  
   Vice Chancellor and Chief Audit Officer

FROM: Timothy P. White  [Signature]
   Chancellor

SUBJECT: Draft Final Report 13-36 on  
   Sensitive Data Security and Protection,  
   Office of the Chancellor

In response to your memorandum of March 4, 2014, I accept the response as submitted with the draft final report on Sensitive Data Security and Protection, Office of the Chancellor.

TPW/amd