SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY,
DOMINGUEZ HILLS

Audit Report 13-34
September 12, 2013

Members, Committee on Audit

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

Staff

University Auditor: 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

Asset Management ........................................................................................................................................ 6
  Protected Data Inventory Assessment ..................................................................................................... 6
  Record Retention and Disposal ................................................................................................................ 7

Human Resources ......................................................................................................................................... 7
  Security Training ..................................................................................................................................... 7
  Confidentiality Agreements ..................................................................................................................... 8

Access Controls ............................................................................................................................................ 9
  Protection of Paper Documents ............................................................................................................... 9
  System Access ....................................................................................................................................... 10

Compliance ................................................................................................................................................. 10

Encryption ................................................................................................................................................... 12
  Storage of Protected Data ....................................................................................................................... 12
  Transmission of Protected Data ............................................................................................................. 13
APPENDICES

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

ABBREVIATIONS

AVP  Associate Vice President
CSU  California State University
CSUDH California State University, Dominguez Hills
EO   Executive Order
ICSUAM Integrated California State University Administrative Manual
ISO  Information Security Office
IT   Information Technology
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor 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 the University Auditor had previously reviewed sensitive data at six campuses in the 2011.

We visited the California State University, Dominguez Hills campus from April 30, 2013, through May 20, 2013, and audited the procedures in effect at that time.

In our opinion, except for the effect of the weaknesses described below, the fiscal, operational, and administrative controls for sensitive data as of May 20, 2013, taken as a whole, were sufficient to meet the objectives stated above and in the “Purpose” section of this report. Areas of concern include: asset management, human resources, access controls, compliance, and encryption.

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 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.

ASSET MANAGEMENT [6]

The campus did not perform periodic inventory and controls assessments of all protected data maintained for electronic and paper files. Additionally, data records were not consistently disposed of at the end of the required retention period.

HUMAN RESOURCES [7]

The campus did not require all computer information users to complete information security awareness training. Additionally, the campus did not obtain completed data confidentiality agreements from all employees with access to sensitive data.
ACCESS CONTROLS [9]

Physical security of sensitive paper documents was inadequate. Specifically, certain colleges/departments maintained sensitive paper documents in unlocked filing cabinets. Additionally, access to protected information in the medical system was not restricted to only authorized personnel.

COMPLIANCE [10]

The campus had not identified data owners for all types of records.

ENCRYPTION [12]

The campus did not store protected data maintained on mobile devices and applications in an encrypted format. Additionally, the campus did not always transmit protected data to third parties in an encrypted format.
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.
INTRODUCTION

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.
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.
ASSET MANAGEMENT

PROTECTED DATA INVENTORY ASSESSMENT

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

Integrated California State University Administrative Manual (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 California State University (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 associate vice president (AVP) of information technology (IT) stated that the campus did not perform periodic inventory and controls assessments of all protected data maintained in electronic and paper files due to limited resources and time constraints.

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 1

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

Campus Response

We concur. Campus information security will incorporate the identification of paper documents containing protected data with the secure storage and destruction of documents containing level 1 and level 2 data into the campus records retention process.
RECORD RETENTION AND DISPOSAL

Data records were not consistently disposed of at the end of the required retention period.

Executive Order (EO) 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.

The AVP of IT stated that data records were not consistently disposed of at the end of the required retention period because department management was not ensuring that the standards and guidelines provided by the chancellor’s office and California State University, Dominguez Hills (CSUDH) information security office (ISO) were being followed. He also stated that procedures had not been developed to enforce record retention policies.

Retention of records beyond their expiration date could make them subject to public records requests and could lead to unnecessary expenditure for their storage and maintenance.

**Recommendation 2**

We recommend that the campus consistently dispose of all electronic data records at the end of the required retention period.

**Campus Response**

We concur. The campus will put in place a process to assess timely disposal of records as dictated by the CSU records retention policy.

Expected completion date: January 2014

HUMAN RESOURCES

SECURITY TRAINING

The campus did not require all computer information 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 AVP of IT stated that new-hire orientation for employees included training on the protection of confidential information. He also stated that the campus offers regular information security awareness training sessions to all employees, but attendance is voluntary.

Lack of information security awareness training increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could cause the campus to be out of compliance with CSU and statutory information security requirements.

**Recommendation 3**

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

**Campus Response**

We concur. The ISO shall work with campus human resources to formulate a plan to enroll all users into the current CSU security awareness training.

Expected completion date: January 2014

**CONFIDENTIALITY AGREEMENTS**

The campus did not obtain completed data confidentiality agreements from all employees who had access to sensitive data.

Specifically, we found that five of 18 employees hired into sensitive positions, including student assistant positions, did not complete a confidentiality agreement.

ICSUAM §8030, *Personal Information Security*, dated April 19, 2010, states all users are expected to employ security practices appropriate to their responsibilities and roles. Users who access level 1 or level 2 data as defined in the CSU Data Classification Standard must sign an approved systemwide confidentiality (non-disclosure) agreement.

The employment manager stated that confidentiality agreements were not completed for all employees with access to sensitive data due to oversight.

Lack of completed data confidentiality agreements from all employees with access to sensitive data increases the risk of inappropriate disclosure of data and campus exposure to liability for any such disclosures.
Recommendation 4

We recommend that the campus obtain completed data confidentiality agreements from all employees who have access to sensitive data.

Campus Response

We concur. The ISO shall work with campus human resources to formulate a process by which all employees who have access to sensitive data acknowledge the CSU confidentiality agreement as a component of completing the current CSU security awareness training.

Expected completion date: January 2014

ACCESS CONTROLS

PROTECTION OF PAPER DOCUMENTS

Physical security of sensitive paper documents was inadequate.

Specifically, we reviewed seven colleges/departments and found that three maintained sensitive paper documents in unlocked filing cabinets.

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. 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 AVP of IT stated that some of the documents were maintained in unsecured filing cabinets because the general office areas in which the files were located were locked after business hours and were thus considered secure. He further stated that some files were maintained in unsecured cabinets due to space constraints.

Inadequate physical security over paper documents containing sensitive data increases the risk of information security breaches and unauthorized access to sensitive information.

Recommendation 5

We recommend that the campus secure all sensitive paper documents in locked filing cabinets.
**Campus Response**

We concur. The campus will review the existing secure file storage and physical access controls and develop procedures to ensure that sensitive paper documents are secured properly at all times.

Expected completion date: January 2014

**SYSTEM ACCESS**

Access to protected information in the medical system was not restricted to only authorized personnel.

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.

The AVP of IT stated that the vendor-provided application did not provide for the ability to limit who may access specific fields within the record that contained sensitive information.

Improper access to sensitive data could lead to unauthorized or inappropriate exposure to sensitive data and can adversely affect campus compliance with existing regulations regarding protection of such data.

**Recommendation 6**

We recommend that the campus restrict access to protected data in the medical system to only authorized individuals.

**Campus Response**

We concur. The medical system will have all sensitive un-required data redacted or purged. Access to the current medical system will be restricted to only student health center staff specifically approved by the student health center director. Access request and confidentiality statements will be maintained in the student health center.

Expected completion date: January 2014

**COMPLIANCE**

The campus had not identified data owners for all types of records.
EO 1031, Systemwide Records/Information Retention and Disposition Schedules Implementation, dated February 27, 2008, states that each campus must formally designate an official campus custodian for each type of record.

ICSUAM §8065, Information Security Data Classification, 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. Additionally, these assets must have a designated owner whose responsibilities include classification, security requirements and management of their designated information assets.

State Administrative Manual §5320.2 states that the responsibilities of the designated owner of records (paper or electronic, including automated files or databases) consist of eliminating the unnecessary collection, use, and maintenance of personal information in agency records, providing proper notice with the collection of personal information; classifying each record, file, or database for which it has ownership responsibility in accordance with the need for precautions in controlling access to and preserving the security and integrity of the record, file, or database; defining precautions for controlling access to and preserving the security and integrity of records, files, and databases that have been classified as requiring such precautions; authorizing access to the information in accordance with the classification of the information and the need for access to the information; monitoring and ensuring compliance with all applicable laws, and agency and state security policies and procedures affecting the information; identifying for each record, file, or database the level of acceptable risk; reporting security incidents and filing security incidents with the information security office; submitting a breach notification to the information security office for review and approval prior to its dissemination or release to any individuals; and monitoring and ensuring authorized users and custodians are aware of and comply with these responsibilities.

The AVP of IT stated that the heads of each division or department were assumed to be the data owners, but this designation had not been formally documented.

Inadequate identification of data owners for records increases the risk of inadequate security of sensitive data, which could result in exposure of sensitive data, gaps in internal control, or non-compliance with the information security program.

**Recommendation 7**

We recommend that the campus identify data owners for all types of records.

**Campus Response**

We concur. The campus will develop a roles and responsibility standard outlining data ownership and responsibilities.

Expected completion date: January 2014
ENCRYPTION

STORAGE OF PROTECTED DATA

The campus did not store protected data maintained on mobile devices and applications 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. Additionally, each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability. Additionally, 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.

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 AVP of IT stated that some mobile devices were used to store sensitive information without his approval, and as such, IT was not able to ensure that the data was secured, encrypted, and backed up on a daily basis. He also stated that in other cases, vendor-provided applications in use did not provide for encryption technology.

Lack of encryption for protected data in storage 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 8

We recommend that the campus store protected data maintained on mobile devices and applications in an encrypted format.

Campus Response

We concur. The campus will develop and implement business practices and standards describing acceptable use and storage of protected data on mobile devices.

Expected completion date: January 2014
TRANSMISSION OF PROTECTED DATA

The campus did not always transmit protected data to third parties in an encrypted format.

CSUDH *Information Security Presidential Memorandum*, dated November 5, 2009, states that confidential data transferred over networks should be encrypted to ensure security.

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. Additionally, each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. 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 AVP of IT stated that the campus did not always transmit protected data in an encrypted format because department management was not ensuring that the standards and guidelines provided by the CSU and CSUDH ISO were being followed.

Lack of encryption for protected data in transit 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 9**

We recommend that the campus transmit protected data to third parties in an encrypted format.

**Campus Response**

We concur. The campus will develop and implement business practices describing acceptable use and transmission of protected data to third parties.

Expected completion date: January 2014
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willie J. Hag</td>
<td>President</td>
</tr>
<tr>
<td>Ronald Bergmann</td>
<td>Associate Vice President (AVP) of Information Technology</td>
</tr>
<tr>
<td>Benjamin Boish</td>
<td>Manager, Compensation &amp; Training, Human Resources Management</td>
</tr>
<tr>
<td>Alisha Brown</td>
<td>Workers’ Compensation Program Manager</td>
</tr>
<tr>
<td>Rene Castro</td>
<td>Director, Faculty Affairs</td>
</tr>
<tr>
<td>Kathleen Chai</td>
<td>Associate Professor, Nursing</td>
</tr>
<tr>
<td>Constance Chambers</td>
<td>Analyst/Programmer, Student Information Services</td>
</tr>
<tr>
<td>Julia Chan</td>
<td>Payroll Manager</td>
</tr>
<tr>
<td>Catherine Earl</td>
<td>Director, Nursing</td>
</tr>
<tr>
<td>Michael Foo</td>
<td>Operating System Analyst, Server Operations and Administration</td>
</tr>
<tr>
<td>Delores Lee</td>
<td>Director, Financial Aid</td>
</tr>
<tr>
<td>Peter Kim</td>
<td>Director, University Advisement</td>
</tr>
<tr>
<td>Lawrence Kimaara</td>
<td>Manager, Business Process Management</td>
</tr>
<tr>
<td>Jamie Dote-Kwan</td>
<td>Professor, Special Education</td>
</tr>
<tr>
<td>Enola Thompson-Logan</td>
<td>Support Services Administrator, Student Health and Psychological Services</td>
</tr>
<tr>
<td>Danny Lujan</td>
<td>Director of Infrastructure</td>
</tr>
<tr>
<td>Wei Ma</td>
<td>Electronic Resources Management Librarian and Reference</td>
</tr>
<tr>
<td>Janie MacHarg</td>
<td>Director, Student Health and Psychological Services</td>
</tr>
<tr>
<td>Mitchell Maki</td>
<td>Vice Provost, Academic Affairs</td>
</tr>
<tr>
<td>Chris Manriquez</td>
<td>Chief Information Technology Officer</td>
</tr>
<tr>
<td>Juan Mejia</td>
<td>Computing Consultant, Financial Aid</td>
</tr>
<tr>
<td>George McCalmon</td>
<td>Operations Systems Analyst, Administrative Information and Common Management Systems</td>
</tr>
<tr>
<td>Brandy McLelland</td>
<td>Director, Student Information Services and Registrar</td>
</tr>
<tr>
<td>April Mitchell</td>
<td>Academic Resource, College of Education</td>
</tr>
<tr>
<td>Sandra Parham</td>
<td>Dean, Library</td>
</tr>
<tr>
<td>Francisco Quinonez</td>
<td>Director, Procurement, Contracts, Logistical and Support Services</td>
</tr>
<tr>
<td>Jill Richardson</td>
<td>Master’s Entry-level Professional Nursing and Clinical Coordinator</td>
</tr>
<tr>
<td>Mary Ann Rodriguez</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Ormond Rucker</td>
<td>Office Manager, Faculty Affairs</td>
</tr>
<tr>
<td>Steven Sanchez</td>
<td>Operating System Analyst, Server Operations and Administration</td>
</tr>
<tr>
<td>Miya Smith</td>
<td>Assistant to the Deans, College of Natural and Behavioral Sciences</td>
</tr>
<tr>
<td>Rakesha Thomas</td>
<td>Employment Manager</td>
</tr>
<tr>
<td>Sharon Tipple</td>
<td>Clinical Instructor, Nursing</td>
</tr>
<tr>
<td>Karen Wall</td>
<td>AVP, Administration and Finance</td>
</tr>
<tr>
<td>Patricia Wells</td>
<td>Director, Disabled Student Services</td>
</tr>
</tbody>
</table>
October 9, 2013

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

Dear Mr. Mandel:

Enclosed, please find California State University, Dominguez Hills' responses to the Sensitive Data Security and Protection Audit Report 13-34, dated September 12, 2013. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or would like additional information, please contact me.

Sincerely,

Mary Ann Rodriguez  
Vice President, Administration and Finance

Enclosure (1)

c: Willie J. Hagan, President  
Karen Wall, Associate Vice President, Administration and Finance
SENSITIVE DATA SECURITY AND PROTECTION
CALIFORNIA STATE UNIVERSITY,
DOMINGUEZ HILLS
Audit Report 13-34

ASSET MANAGEMENT

PROTECTED DATA INVENTORY ASSESSMENT

Recommendation 1

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

Campus Response

We concur. Campus information security will incorporate the identification of paper documents containing protected data with the secure storage and destruction of documents containing level 1 and level 2 data into the campus records retention process.

Expected completion date: January 2014

RECORD RETENTION AND DISPOSAL

Recommendation 2

We recommend that the campus consistently dispose of all electronic data records at the end of the required retention period.

Campus Response

We concur. The campus will put in place a process to assess timely disposal of records as dictated by the CSU records retention policy.

Expected completion date: January 2014
HUMAN RESOURCES

SECURITY TRAINING

Recommendation 3

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

Campus Response

We concur. The information security office shall work with campus human resources to formulate a plan to enroll all users into the current CSU security awareness training.

Expected completion date: January 2014

CONFIDENTIALITY AGREEMENTS

Recommendation 4

We recommend that the campus obtain completed data confidentiality agreements from all employees who have access to sensitive data.

Campus Response

We concur. The information security office shall work with campus human resources to formulate a process by which all employees who have access to sensitive data acknowledge the CSU confidentiality agreement as a component of completing the current CSU security awareness training.

Expected completion date: January 2014

ACCESS CONTROLS

PROTECTION OF PAPER DOCUMENTS

Recommendation 5

We recommend that the campus secure all sensitive paper documents in locked filing cabinets.

Campus Response

We concur. The campus will review the existing secure file storage and physical access controls and develop procedures to ensure that sensitive paper documents are secured properly at all times.

Expected completion date: January 2014
SYSTEM ACCESS

Recommendation 6

We recommend that the campus restrict access to protected data in the medical system to only authorized individuals.

Campus Response

We concur. The medical system will have all sensitive un-required data redacted or purged. Access to the current medical system will be restricted to only student health center staff specifically approved by the student health center director. Access request and confidentiality statements will be maintained in the student health center.

Expected completion date: January 2014

COMPLIANCE

Recommendation 7

We recommend that the campus identify data owners for all types of records.

Campus Response

We concur. The campus will develop a roles and responsibility standard outlining data ownership and responsibilities.

Expected completion date: January 2014

ENCRYPTION

STORAGE OF PROTECTED DATA

Recommendation 8

We recommend that the campus store protected data maintained on mobile devices and applications in an encrypted format.

Campus Response

We concur. The campus will develop and implement business practices and standards describing acceptable use and storage of protected data on mobile devices.

Expected completion date: January 2014
TRANSMISSION OF PROTECTED DATA

Recommendation 9

We recommend that the campus transmit protected data to third parties in an encrypted format.

Campus Response

We concur. The campus will develop and implement business practices describing acceptable use and transmission of protected data to third parties.

Expected completion date: January 2014
October 21, 2013

**MEMORANDUM**

**TO:** Mr. Larry Mandel  
University Auditor

**FROM:** Timothy P. White  
Chancellor

**SUBJECT:** Draft Final Report 13-34 on  
*Sensitive Data Security and Protection*,  
California State University, Dominguez Hills

In response to your memorandum of October 21, 2013, I accept the response as submitted with the draft final report on *Sensitive Data Security and Protection*, California State University, Dominguez Hills.

TPW/amd