Sensitive Data Control Plans

Texas Center for Learning Disabilities – Project 1

December 2014

The University of Texas at Austin
Office of Internal Audits
UTA 2.302
(512) 471-7117
The University of Texas at Austin
Internal Audit Committee

Mr. William O'Hara, Independent Member, Chair
Mr. William C. Powers Jr., President
Dr. Gregory Fenves, Executive Vice President and Provost
Mr. Kevin P. Hegarty, Vice President and Chief Financial Officer
Dr. Patricia L. Clubb, Vice President for University Operations
Ms. Patricia C. Ohlendorf, Vice President for Legal Affairs
Dr. Juan M. Sanchez, Vice President for Research
Dr. Gage F. Paine, Vice President for Student Affairs
Ms. Mary E. Knight, CPA, Associate Vice President
Mr. Paul Liebman, Chief Compliance Officer, University Compliance Services
Mr. Cameron D. Beasley, University Information Security Officer
Mr. Tom Carter, Independent Member
Ms. Lynn Utter, Independent Member
Mr. Michael W. Vandervort, Director, Office of Internal Audits
Mr. J. Michael Peppers, Chief Audit Executive, University of Texas System

The University of Texas at Austin
Office of Internal Audits

Director: Michael Vandervort, CPA
Associate Director: Jeff Treichel, CPA
Assistant Directors:
  * Angela McCarter, CIA, CRMA
  * Chris Taylor, CIA, CISA
Auditor III:
  * Ashley Foster, CPA
  * Cameosha Jones
  * Cynthia Martin-Hajmasy, CPA
Auditor II:
  * Miranda Pruett, CFE
Auditor I:
  * Stephanie Grayson
  * Kerri Jordan
  * Bobby Castillo
Sr. IT Auditor:
  * Tod Maxwell, CISA, CISSP
IT Auditor:
  * Brandon Morales, CISA, CGAP
  * Amber Whelpley, CIA, CGAP

* denotes project members

This report has been distributed to Internal Audit Committee members, the Legislative Budget Board, the State Auditor’s Office, the Sunset Advisory Commission, the Governor’s Office of Budget and Planning, and The University of Texas System Audit Office for distribution to the Audit, Compliance, and Management Review Committee of the Board of Regents.

Sensitive Data Control Plans
Project Number: 14.303
December 1, 2014

President William C. Powers, Jr.
University of Texas at Austin
Office of the President
P.O. Box T
Austin, Texas 78713

Dear President Powers,

We have completed our audit of the Sensitive Data Control Plan (SDCP) for Project: Texas Center for Learning Disabilities – Project 1. Our scope included SDCPs put in place during fiscal year 2014.

Based on a review of SDCP requirements and supporting documentation, interviews with relevant staff members, and limited testing, it appears that the SDCP is being followed, sensitive data is sufficiently secured, and the Threat Model completed by the Principal Investigator is correct. Our audit report provides detailed observations for each area under review. One suggestion is offered in the report for improvement in the existing control structure.

We appreciated the cooperation and assistance of those associated with this project in the College of Education throughout the audit and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA
Director

cc: Internal Audit Committee Members
Dr. Gregory Roberts, Director IV, Meadows Center and Vaughn Gross Center, College of Education
Dr. Susan Sedwick, Associate Vice President for Research and Director, Office of Sponsored Projects
Ms. Nancy Brazzil, Deputy to the President and Chief of Staff
TABLE OF CONTENTS

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

Background ...................................................................................................................... 2

Scope, Objectives, and Procedures .................................................................................. 2

Audit Results ..................................................................................................................... 3

Conclusion ....................................................................................................................... 4
EXECUTIVE SUMMARY

This audit was conducted as part of the Fiscal Year 2014 Audit Plan and based on risk identified in the annual risk assessment. The scope of this audit included a Sensitive Data Control Plan (SDCP) put in place during fiscal year 2014. Our objectives were to determine whether:

- The area under review is following the SDCP,
- The sensitive data is sufficiently secured, and
- The Threat Model completed by the Principal Investigator appears to be correct.

The Office of Sponsored Projects has developed an SDCP template to document the procedures that will be utilized to protect sensitive research data. The Information Security Office provides assistance by reviewing SDCPs at the beginning of a project. If the project is externally sponsored, it must be approved by the director of the Office of Sponsored Projects. In the event that sensitive data is acquired in an agreement that is not externally sponsored, it is the responsibility of the College to execute agreements that will adequately protect the data.

Internal Audits worked with the Office of Sponsored Projects and the Information Security Office to select the project titled Texas Center for Learning Disabilities – Project 1 as the focus of this audit. The principal investigator/responsible individual for this project conducts research in association with The Meadows Center and the Vaughn Gross Center for Reading and Language Arts in the College of Education. The “restricted-use” licensed data is provided by the Institute of Education Sciences and the project is sponsored by the National Institutes of Health.

Based on a review of SDCP requirements and supporting documentation, interviews with relevant staff members, and limited testing, it appears that the SDCP is being followed, sensitive data is sufficiently secured, and the Threat Model completed by the principal investigator is correct. One recommendation was made to maintain compliance with IT Policy. Management agreed with the recommendation and has taken corrective action.

---

1The Threat Model is a self-evaluation completed by the Principal Investigator with assistance from the Office of Sponsored Projects intended to identify the probability that different individuals would be able to access sensitive data physically and/or over a network.
BACKGROUND

In a memorandum addressed to deans of The University of Texas at Austin, the Vice President for Research explained that “The Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) established uniform policy for confidentiality protection of statistical information collections sponsored or conducted by more than 70 Federal agencies. Information that can be used to distinguish or track an individual’s identity such as name, Social Security Number, or biometric information as well as information that could be used in conjunction with other data elements to reasonably infer the identity of a respondent such as a combination of gender, race, date of birth, geographic indicators, or other descriptors is protected. Special procedures are required for use of laptop computers, PDAs, zip drives, floppy disks, CD-ROMs or any other IT devices.”

In response to this policy, The Office of Sponsored Projects has developed a template Sensitive Data Control Plan (SDCP) form to document the procedures that will be utilized to protect covered information. The Information Security Office provides assistance by reviewing SDCPs at the beginning of a project. If the project is externally sponsored, it must be approved by the director of the Office of Sponsored Projects. In the event that sensitive data is acquired in an agreement that is not externally sponsored, it is the responsibility of the College to execute agreements that will adequately protect the data.

The Office of Internal Audits (IA) worked with the Office of Sponsored Projects and the Information Security Office to select the project titled Texas Center for Learning Disabilities – Project I as the focus of this audit.

The principal investigator (PI)/responsible individual for this project conducts research in association with The Meadows Center and the Vaughn Gross Center for Reading and Language Arts in the College of Education. The “restricted-use” student data is provided by the Institute of Education Sciences and the project is sponsored by the National Institutes of Health.

SCOPE, OBJECTIVES, AND PROCEDURES

The scope of this audit included an SDCP put in place during fiscal year 2014. Our objectives were to determine whether:

- The area under review is following the SDCP,
- The sensitive data is sufficiently secured, and
- The Threat Model completed by the Principal Investigator appears to be correct.

---

2 Memorandum from the Vice President for Research - http://www.utexas.edu/research/osp/documents/data_use_agreements.pdf
To achieve these objectives, IA:

- Reviewed SDCP requirements,
- Conducted interviews with relevant staff members,
- Reviewed supporting documentation, and
- Conducted limited testing.

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and with *Government Auditing Standards*.

The remainder of this report presents detailed observations and recommendations.

**AUDIT RESULTS**

IA gained an understanding of SDCPs in general and then chose the SDCP created for the *Texas Center for Learning Disabilities – Project 1* to be audited.

The term of the license allows the use of sensitive data for five years from March 2014 with an option for the dates to be amended. The sensitive data was provided to the PI and is secured in an office on campus within the College of Education. Only one desktop computer was used to access the sensitive data and it was not connected to a network.

One recommendation was made to maintain compliance with UT Austin IT policy.

**Position of Special Trust Form**

The PI for the project has administrative privileges on the computer used to access sensitive data and had not completed a Position of Special Trust form until discussed at a meeting with IA. The PI’s position is not flagged as a position of special trust in the Human Resource Management System; therefore he was not aware that he needed to complete the form.

According to the Information Security Office website, “in accordance with The University of Texas at Austin Information Resources Use and Security Policy (section V, item 4), all university employees with elevated systems privileges and access to Category-I university data shall be required to acknowledge annually the additional responsibilities they bear with those privileges by signing a Position of Special Trust form.”

Without completing the Position of Special Trust form annually, employees may not be aware of their responsibilities for handling Category I data. This could lead to a loss or misuse of UT Austin data and/or a loss of revenue in the event of a compromise.
**Recommendation:** The PI for the project should ensure that his position is designated as a Position of Special Trust form in the Human Resource Management System and should complete the form annually.

**Management’s Corrective Action Plan:** Management will ensure that the PI’s position is designated as a position of special trust in the Human Resource Management System.
Responsible Person: Principal Investigator for the project
Planned Implementation Date: Immediately

**Post Audit Review:** Internal Audits has verified that the PI’s position has been designated as a position of special trust in the Human Resource Management System as of 11/13/2014.

**CONCLUSION**

Based on a review of SDCP requirements and supporting documentation, interviews with relevant staff members, and limited testing, it appears that the SDCP is being followed, sensitive data is sufficiently secured, and the Threat Model\(^3\) completed by the Principal Investigator is correct. One recommendation was made to maintain compliance with IT Policy.

---

\(^3\) The Threat Model is a self-evaluation completed by the Principal Investigator with assistance from the Office of Sponsored Projects intended to identify the probability that different individuals would be able to access sensitive data physically and/or over a network.