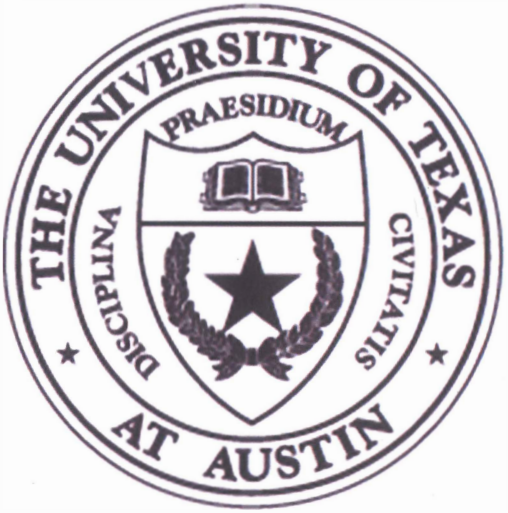
Sensitive Data Control Plans

Romantic Partner Consensus



August 2015

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
Dr. Gregory L. Fenves, President
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 E. Paine, Vice President for Student Affairs
Ms. Mary E. Knight, CPA, Associate Vice President and Interim Chief Financial Officer
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
Audit Manager:	*Brandon Morales, CISA, CGAP
Auditor III:	Michael Hammond, CIA, CISA, CFE Cynthia Martin-Hajmasy, CPA Ashley Oheim, CPA
Auditor II:	Stephanie Grayson Miranda Pruett, CFE
Auditor I:	Jason Boone Bobby Castillo Kerri Jordan
Sr. IT Auditor:	Tod Maxwell, CISA, CISSP
IT Auditor	Tiffany Yanagawa

* 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: 15.307

OFFICE OF INTERNAL AUDITS
THE UNIVERSITY OF TEXAS AT AUSTIN

1616 Guadalupe Street, Suite 2.302 • Austin, TX 78701 • (512)471-7117 • FAX (512)471-8099

August 19, 2015

President Gregory L. Fenves
The University of Texas at Austin
Office of the President
P.O. Box T
Austin, Texas 78713

Dear President Fenves,

We have completed our audit of the Sensitive Data Control Plan (SDCP) for the Romantic Partner Consensus research project. Our scope included the SDCP for the research project.

Based on audit procedures performed, 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. Suggestions are offered throughout the report for improvement in the existing control structure.

We appreciate the cooperation and assistance of the Principal Investigator for the project throughout the audit and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA
Director

cc: Internal Audit Committee Members
Dr. Paul Eastwick, Assistant Professor, Human Development and Family Science, College of Natural Sciences
Mr. Jason Richter, Interim Director, Office of Sponsored Projects
Mr. Jeff Treichel, Associate Director, Office of Internal Audits

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Conclusion

Based on audit procedures performed, it appears that the Sensitive Data Control Plan (SDCP) is being followed, sensitive data is sufficiently secured, and the Threat Model[1] completed by the Principal Investigator is correct. Three recommendations were made to maintain compliance with IT policies and requirements.

Summary of Recommendations

Each issue has been ranked according to The University of Texas System Administration Audit Issue Ranking guidelines. Please see Appendix for ranking definitions. Internal Audits identified one notable issue which led to the following recommendation:

- Ensure that the computer used to store and access sensitive data is either physically locked down by a cable attaching it to the desk or by a locking cabinet specifically designed for this purpose. (Audit Finding Ranking: High)

Two additional recommendations are also provided, but are considered minor in significance. Management agreed with our observations and has provided corrective action plans which are expected to be implemented on or before August 31, 2015.

Audit Scope and Objective

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.

Background Summary

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.

Internal Audits worked with the Office of Sponsored Projects and the Information Security Office to select a project titled *Romantic Partner Consensus* as the focus of this audit. The Principal Investigator/responsible individual for this project conducts research in association with the department of Human Development and Family Science in the College of Natural Sciences. The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) protected data is provided by The University of Michigan and the project is sponsored by the National Longitudinal Study of Adolescent Health. This audit was conducted as part of the Fiscal Year 2015 Audit Plan and was based on risk identified in the 2014 annual risk assessment.

[1] 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.

BACKGROUND

In a memorandum addressed to deans of The University of Texas at Austin (UT 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."[2]

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 research project. In 2014, research projects that were externally sponsored required approval by the director of the Office of Sponsored Projects. When an agreement was not externally sponsored, the College was responsible for executing agreements to adequately protect the data.

The Office of Internal Audits (IA) worked with the Office of Sponsored Projects and the Information Security Office to select a research project titled *Romantic Partner Consensus* as the focus of this audit.

The Principal Investigator/responsible individual for this research project conducts research in association with the department of Human Development and Family Science in the College of Natural Sciences. The CIPSEA protected data is provided by The University of Michigan and the research project is sponsored by the National Longitudinal Study of Adolescent Health. This audit was conducted as part of the Fiscal Year 2015 Audit Plan and was based on risk identified in the 2014 annual risk assessment.

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

[2] Memorandum from the Vice President for Research - http://www.utexas.edu/research/osp/documents/data_use_agreements.pdf

- The Threat Model completed by the Principal Investigator (PI) appears to be correct.

To achieve these objectives, IA:

- Reviewed SDCP requirements,
- Interviewed relevant staff,
- 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 *Romantic Partner Consensus* project to be audited.

The term of the contract allows the use of sensitive data for three years from the initiation date in 2014. The sensitive data was provided to the PI and is secured in an office on campus within the Sarah M. and Charles E. Seay Building. Only one desktop computer is used to access the sensitive data and it is not connected to a network.

Three recommendations were made to maintain compliance with IT policies and requirements. Each issue has been ranked according to The University of Texas System Administration Audit Issue Ranking guidelines. Please see the Appendix for ranking definitions.

Physical Security
Audit Issue Ranking: High
The computer used to store and access sensitive data has a lock on it but is not physically locked to the desk with a cable or housed in a locking cabinet. The PI for the project believed that the computer was physically secured by locking the outer housing of the computer itself.

The Computer System and Use Requirements section of *The University of Michigan, Inter-university Consortium for Political and Social Research (ICPSR), National Longitudinal Study of Adolescent Health Sensitive and Romantic Data Contract* requires that "The CPU is physically locked down by either a cable attaching it to the desk or by a locking cabinet specifically designed for this purpose."

Without the required physical security in place, there is an increased risk that sensitive data may be lost or stolen.

Recommendation #1: The PI for the research project should ensure that the computer is either physically locked down by a cable attaching it to the desk or by a locking cabinet specifically designed for this purpose.

Management's Response and Corrective Action Plan:
I will purchase a locking cable for this computer and use the cable to secure the computer to the desk.

Responsible Person: Paul Eastwick
Planned Implementation Date: 8/31/15

Post Audit Review: IA will follow-up in the first quarter of FY16.

Position of Special Trust Form
Audit Issue Ranking: Medium
The PI for the research project has access to sensitive data but has not completed a Position of Special Trust form. The PI's position is not flagged as a position of special trust in the Human Resource Management System; therefore the PI was not aware that the form needed to be completed.

The Information Security Office website states, "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 #2: The PI for the research project should ensure that his position is designated as a position of special trust in the Human Resource Management System and should complete the form on an annual basis.

Management's Response and Corrective Action Plan:
I have now signed the position of special trust form. The HR person is out of the office now but has been contacted to change the designation to a position of special trust in HRMS when she gets back.

Responsible Person: Paul Eastwick
Planned Implementation Date: 8/15/15

Post Audit Review: Implemented - Verified

Log-on Banner
Audit Issue Ranking: Medium
There is no log-on banner present for the authorized user to acknowledge and agree to abide by UT Austin policies upon logging onto the computer. The log-on banner was not added to the computer when it was set up.

Section 4.5.10 of the *Minimum Security Standards for Systems* states that for all systems with access to Category I data, "The required university warning banner should be installed."

Without the proper log-on banner, those accessing the system might not be aware of the restrictions and responsibilities inherent in data use.

Recommendation #3: The PI should ensure that a log-on banner is present when logging on in accordance with the UT Austin *Minimum Security Standards for Systems*.

Management's Response and Corrective Action Plan:
I will install the logon banner text so it appears when I log into the computer.

Responsible Person: Paul Eastwick
Planned Implementation Date: 8/31/15

Post Audit Review: IA will follow-up in the first quarter of FY16.

CONCLUSION

Based on audit procedures performed, 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. Three recommendations were made to maintain compliance with IT policies and requirements.

In accordance with directives from The University of Texas System Board of Regents, the Office of Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

[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.

APPENDIX

Audit Issue Ranking

Audit issues are ranked according to the following definitions, consistent with UT System Audit Office guidance. These determinations are based on overall risk to UT System, UT Austin, and/or the individual college/school/unit if the issues are left uncorrected. These audit issues and rankings are reported to UT System directly.

- ***Priority*** – A Priority Issue is an issue that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Austin or the UT System as a whole.
- ***High*** – An issue that is considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.
- ***Medium*** – An issue that is considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.
- ***Low*** – An issue that is considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level. Issues with a ranking of "Low" are reported verbally to the unit and are not included in the final report.