TEXAS
The University of Texas at Austin

Confidential Data Control Plans

Office of Sponsored Projects

August 2025

Office of Internal Audits
UT Austin's Agents of Change

OFFICE OF INTERNAL AUDITS
THE UNIVERSITY OF TEXAS AT AUSTIN

1616 Guadalupe St. Suite 2.302 · Austin, Texas 78701 · (512) 471-7117
audit.utexas.edu • internal.audits@austin.utexas.edu

Executive Summary

Confidential Data Control Plans

Office of Sponsored Projects
Project Number: AUS25AS0003

Audit Objective

The objective of the audit was to evaluate processes for development and monitoring of Confidential Data Control Plans (CDCPs) and assess whether identified data is handled in conformance with CDCP requirements.

Conclusion

The research labs we observed have technology setups that generally comply with CDCP requirements[1]; however, the processes for developing and monitoring CDCPs are outdated and do not provide centralized oversight, consistent recordkeeping, or clear guidance for principal investigators.

Audit Observations[2]

Recommendation	Risk Level	Estimated Implementation Date
Confidential Data Control Plans Process	High	September 2026

Engagement Team[3]

Ms. Suzi Nelson, CPA, CIA, CISA, Principal Auditor
Mr. Alex Zhang, Auditor
Ms. Molly Grant, Manager, EAG Gulf Coast, LLC

[1] Nine research labs were reviewed across various colleges, schools and units.
[2] Each observation has been ranked according to The University of Texas System Administration (UT System) Audit Risk Ranking guidelines. Please see the last page of the report for ranking definitions.
[3] This project was co-sourced with EAG Gulf Coast, LLC.

Background

In 2005, the Information Security Office (ISO) established CDCPs to document data protection measures during a period when research data was transitioning rapidly from physical to digital formats. Because digital security practices were emerging, and research activity was limited in scale at the time, the ISO directly supported each technology setup required to meet the standards for handling confidential data.

Notable Practice

Principal investigators displayed high awareness of the need to protect confidential data related to human subject research activities.

In 2012, the CDCP process was revised to confirm shared responsibility for data protection between the principal investigators (PIs) and their respective college, school or unit information technology (CSU IT) department. Additionally, the Office of Sponsored Projects (OSP) assumed administrative oversight of the CDCP process. Since then, the compliance monitoring process has become ineffective, and there have been multiple key leadership transitions. Moreover, technological capabilities have advanced, and the CDCP standards have not been updated accordingly.

Although enterprise-level controls implemented by the ISO have reduced institutional risk, they are not designed to fully account for the varied, localized technology setups managed by PIs and CSU IT teams.

Detailed Audit Results

Observation #1 Confidential Data Control Plan Process

The confidential data control plan process is outdated and provides insufficient guidance for PIs, with no centralized oversight or consistent recordkeeping. Key terms that guide CDCP implementation, such as “confidential” and “proprietary,” are broadly defined, resulting in varied interpretations by personnel who are not technical experts in data classification standards. Differences in guidance across the University contribute to the inconsistent application of CDCP requirements, including in response to external data sharing agreements. Existing forms are not aligned with current technologies, and a process has not been established to consistently monitor CDCP updates, closure, or compliance.

Without clear definitions of confidential data, standardized policies, technical resources for both data classification and continuing support, and an ongoing monitoring process, risks are heightened that PIs may fail to protect confidential data.

Management’s Corrective Action Plan:

CDCPs will be included within Controlled Research Oversight, an inter-office collaboration under the direction of the Vice President of Technology and Chief Information Officer. This initiative is designed to ensure appropriate protection and compliance with research data security requirements. While exact steps will be finalized as this program is built, an initial response plan is outlined below to ensure that development and ongoing monitoring of CDCPs is systematic, compliant, and managed by dedicated personnel.

1. OSP or Collaborative Research will identify the need for a CDCP and initiate an ancillary review to Office of Research Support & Compliance (ORSC) Restricted Research.
2. ORSC Restricted Research will act as a liaison between the PI, Enterprise Technology, and the ISO to facilitate CDCP development in accordance with relevant requirements, policies, and procedures.
3. CDCPs will be signed by research team members, ORSC Restricted Research, and ISO.
4. A compliance monitoring position established in ISO will oversee ongoing adherence to the CDCP requirements.

Responsible Persons:

Associate Director for Collaborative Research
Associate Vice President for Research Administration
Associate Vice President, Office of Research Support & Compliance
Vice President of Technology and Chief Information Officer
Chief Information Security Officer

Planned Implementation Date: September 1, 2026

Conclusion

While the research labs observed have technology setups that generally comply with CDCP requirements, the processes for development and monitoring of CDCPs are outdated and do not provide centralized oversight, consistent recordkeeping, or clear guidance for PIs.

Table: Controls Assessment

Audit Objective	Controls Assessment
Evaluate processes for development and monitoring of CDCPs.	Ineffective
Assess whether identified data is handled in conformance with CDCP requirements.	Generally effective

Scope, Objectives, and Methodology

This audit was conducted in conformance with The Institute of Internal Auditors' Global Internal Audit Standards. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards and meet the independence requirements for internal auditors. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.
The scope of this review included CDCPs in place as of March 2025.

Specific audit objectives and the methodology to achieve the objectives are outlined in the table below.

Table: Objectives and Methodology

Audit Objective	Methodology
Evaluate processes for development and monitoring of CDCPs and assess whether identified data is handled in conformance with CDCP requirements.	• Reviewed related policies and procedures. • Interviewed personnel in departments involved in the CDCP process, including OSP, ISO, CSU IT, and PIs. • Examined CDCPs to verify inclusion of controls required by UT policy. • Reviewed Data Use and Licensing Agreements from external parties and associated CDCPs, as applicable. • Conducted design walkthroughs to verify whether technology setups align with CDCP requirements.

Criteria

- UT Austin Information Resources and Use Security Policy
  - Standard 9 – Data Classification
- OSP process and procedures for CDCP administration

Observation Risk Ranking

Audit observations are ranked according to the following definitions, consistent with UT System Audit Office guidance.

Risk Level	Definition
Priority	If not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of The University of Texas at Austin (UT Austin) or the UT System as a whole.
High	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	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	Considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.

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

Report Submission

We appreciate the courtesies and cooperation extended throughout the audit.

Respectfully Submitted,

Sandy Sutton Jansen

Sandy Jansen, CIA, CCSA, CRMA, Chief Audit Executive

Distribution

Mr. James E. Davis, President
Mr. Cam Beasley, Chief Information Security Officer
Mr. Cole Camplese, Vice President of Technology and Chief Information Officer
Mr. Drayton Cullen, Chief of Staff, Office of the Executive Vice President and Provost
Mr. Mark Featherston, Associate Vice President for Research Administration
Mr. Jeff Graves, Chief Compliance Officer
Dr. William Inboden, Executive Vice President and Provost
Ms. Rebecca Leamon, Associate Director for Collaborative Research
Dr. Fernanda Leite, Interim Vice President for Research
Ms. Christy Sobey, Director of President's Office Operations
Dr. Michelle Stickler, Associate Vice President, Office of Research Support and Compliance
The University of Texas at Austin Institutional Audit Committee
The University of Texas System Audit Office
Legislative Budget Board
Governor’s Office
State Auditor’s Office