CONFIDENTIAL DATA CONTROL PLAN (CDCP)

OFFICE OF SPONSORED PROJECTS (OSP)
THE UNIVERSITY OF TEXAS AT AUSTIN

Date Prepared	
CDCP #	*(Assigned by OSP)*

Responsible Individual / Principal Investigator

Name	
Job Title	
UT EID	
Email	
Phone	

Project Information

Sponsored Project?	☐ Yes, this relates to a Sponsored Project.
OSP #	
IRB Protocol #	*If excluded from IRB review, please attach a copy of the ORS documentation.*
Data Provider	
Project Title	

Attachments

1. Confidential Data Control Plan (CDCP)
2. Certification on the Handling of Confidential Data
   Each individual subject to this CDCP must submit a separate Certification.

Approvals

Responsible Individual / Principal Investigator Signature	
Name	
Job Title	
Date	

Local IT Administrator Signature	
Name	
Job Title	
Date	

CONFIDENTIAL DATA CONTROL PLAN (CDCP)

Overview

The University of Texas at Austin (UT Austin) is committed to compliance and the protection of Confidential Data whether in hard copy or digital format. The Office of Sponsored Projects (OSP), in consultation with the Information Security Office, maintains oversight and record of Confidential Data Control Plans (CDCPs) on behalf of the University.

It is important to note that this CDCP is project-specific and is, therefore, only applicable to the project identified on this form.

It is the duty of the above named Responsible Individual/Principal Investigator (PI) to ensure compliance with this CDCP and to inform OSP of any changes to personnel, equipment, devices, or services used in storing Confidential Data not included within this plan and to submit additional documentation, as necessary.

After consultation with local IT support, please contact the Information Security Office for questions and assistance at iso@austin.utexas.edu.

Describe the specific circumstances that require the use of this Confidential Data:

Physical and Logical Security

The University of Texas System rules require all researchers safeguard and protect sensitive research data, otherwise classified as Confidential Data under the Data Classification Standard.

Because of the risk, the use of laptops, mobile devices, or other external storage devices for the storage of this Data must be justified and must undergo additional security measures, such as encryption, as outlined by University policy.

Any University servers used for this research must be located in the University Data Center, per University policy, unless the Information Security office has approved a security exception request.

PI should respond to all of the following questions in consultation with their local IT Support Teams. When describing a process, please try to describe the controls as completely as possible. For example, if any specific products or technologies will be used to comply with these requirements, mention them by name and be as specific as possible when describing how they will be used.

Each question below is linked to a specific policy or legal requirement with which compliance is mandatory. Links to reference documents are provided following the questions. Specific agreements may require additional protections; those additional protective measures may be included in-line with the answers to other questions, or may be added at the end of this section.

The following are abbreviations used within the document for reference:

- DEG Data Encryption Guidelines
- HDD Hard Drive Destruction
- MSSDS Minimum Security Standards for Data Stewardship
- MSSS Minimum Security Standards for Systems
- MDHC Multifunction Device Hardening Checklist

If Confidential Data will be stored on University property, where will it be located?

Building	
Room	

If there is an offsite backup of the Data, where will it be located?

Building	
Room	

If the Confidential Data will be transmitted over a wired, wireless, or cellular network, please describe how it will be transmitted. Describe the methods being used to encrypt or otherwise protect the Data in transit: (MSSDS 4.3-4; MSSS 4.5.6-7; DEG)

If the Confidential Data is accessible by any device(s) connected to a network, how will the devices be protected from unauthorized access via the network? If the network has any unique features, such as limited access, please briefly describe them: (MSSS 4.5)

Please describe how desktop computers will be physically secured. Examples include screen locks that apply automatically after 15 minutes of inactivity, encrypted hard drives, locked offices, and so on. (MSSS 4.4)

Please describe how will printers and other output devices be physically secured. (MDHC 18-21)

Please describe how servers will be physically secured. Examples include Building Access Control System (BACS) proximity cards, University-managed surveillance cameras, motion alarms, and so on. (MSSS 4.4)

Please describe how the Confidential Data will be secured from the access/viewing of unauthorized individuals? Please address both the copying of the Data from devices and the viewing of the Data on devices such as computer displays:

If the Confidential Data will be printed, faxed, or otherwise output, describe how the physical output will be protected. This includes protection while being printed/waiting for pickup, during use, during storage, and when being disposed of. (MSSDS 4.2)

If the Confidential Data will be stored on a portable/mobile device, or on removable media, where will the device or media be stored and used? Please describe how the Data will be secured on the device and/or media. How will devices and media handling Confidential Data be disposed of? (MSSDS 4.3; MSSS 4.4, 4.5.7, 4.5.11)

Please describe how these systems will be managed by a local IT support group or otherwise professionally managed according to campus IT policy. Include system management procedures, tools, and the names/EIDs and qualifications of the individuals responsible for system management:

In accordance with University policy, all desktop computers, portable computing devices (such as laptops), and portable/removable media must be encrypted. Servers may also require encryption if physical security controls are weak or of concern.

Please indicate how this Data will be encrypted. What steps (for example, using Stache or UT Backup) will be taken to ensure that the Data is recoverable in the event that an encryption key is lost or forgotten?

Please provide all of the wired and wireless media access control (MAC) addresses of the laptops, desktops, and servers to be used. Please also note which person(s) is associated with each of these devices:

MAC Address 1	Person(s)

Please describe any additional protective measures not already mentioned:

Personnel Screening

All personnel with access to the Data must complete the *Certification on the Handling of Confidential Data* and must be named in this document.

All personnel must complete the Acceptable Use Policy Acknowledgment Form every year as long as the project is active or the Data is being retained.

Insert any information on the type of background check and any additional required reviews that will be administered (beyond the standard background check procedures) to the individuals with access to the Data:

Training and Awareness

All personnel with access to Confidential Data must read and agree to abide by the UT Austin policy on protecting Confidential Data and any special requirements listed in this Plan regarding the protection of the Data.

All personnel with access to Confidential Data must complete the online Security Awareness compliance training module every two (2) years.

Compliance Assessment

As a critical component of UT Austin's ongoing compliance monitoring, self-evaluation shall be conducted and all persons with access to this Data agree to cooperate fully.

Any potential or actual security breach of protected Data must immediately be reported to the Responsible Individual/Principal Investigator; the Information Security Office, by email to security@utexas.edu; and the Office of Sponsored Projects, by email to osp@austin.utexas.edu.

Changes and Updates

Prior to additional personnel gaining access to the Confidential Data identified herein, the Responsible Individual/PI must submit to OSP a separate *Certification on the Handling of Confidential Data* signed by each added person.

A revised CDCP form is required for the addition or changes to equipment, devices, or services to be used for the storage of the Confidential Data not included in the original plan. Please submit all changes to OSP by email at osp@austin.utexas.edu.

Follow-Up Review

The Information Security Office, Internal Audit, and/or the Office of Sponsored Projects reserve the right to conduct follow-up reviews or security assessments of work processes or systems associated with this Plan.

Project Termination

Security measures will remain in effect after the project has ended in order to protect the sensitive Data, unless earlier terminated in the case of the Data being destroyed or returned. Additionally, the University reserves the right to terminate this project in the event that this plan is not followed, negligence is identified, or other risks emerge that become unacceptable.

References

- Acceptable Use Policy Acknowledgment Form
- Data Classification Standard
- Data Encryption Guidelines (DEG)
- Hard Drive Destruction
- Minimum Security Standards for Data Stewardship (MSSDS)
- Minimum Security Standards for Systems (MSSS)
- Multifunction Device Hardening Checklist (MDHC)
- Security Awareness Compliance Training Module
- Security Exception Request Form
- Stache (Secure Escrow Service)
- UT Backup

CERTIFICATION ON THE HANDLING OF CONFIDENTIAL DATA

Each individual subject to the Confidential Data Control Plan (CDCP) must submit a separate Certification.

Overview

Insert important details of the CDCP that provide an overview of the access to, use of, and protection of the Confidential Data:

Reasonable Care

Researchers will be held personally liable for violations related to Confidential Data as set forth on this form and in the CDCP.

Penalties

Both civil and criminal penalties may be imposed for noncompliance.

Certification

I hereby certify that I have read and understand this Certification and agree to abide by the Confidential Data controls set forth in the “Physical and Logical Security” section of the CDCP and by the Acceptable Use and Security Policy Agreement (electronically acknowledged annually).

I understand that I may be held personally liable if I breach the procedures outlined herein by disclosing, regardless of form or format, Confidential Data covered under this Certification to unauthorized persons.

Name	
Job Title	
Department	
Project Title	
Data Provider	
Signature	
Date	