**Columbia University Information Technology - Secure Data Enclave (CUIT-SDE)**

**Computing System User Agreement**

This Agreement is between the Columbia University Information Technology group (CUIT) at Columbia University and *SDE User Name (SDE Username)****.*** This Agreement is effective as of *start date* and expires on *end date* unless extended by mutual consentof the data granting agency and CUIT.

CUIT-SDE staff authorize the members of this agreement to access the Secure Data Enclave (SDE) system under the conditions and limitations listed below:

* The Researcher is authorized to access only the confidential data listed below residing in the folders (and subfolders) on the SDE system listed below, in accordance with the data user permissions set by the CUIT-SDE Administrators.

Confidential Data: *name of dataset*

Folder Name: *folder\_location*

* The Researcher agrees not to allow anyone else to use her/his credentials to access the SDE system and is reminded that sharing credentials violates university policy.
* The Researcher agrees not to remove or request removal of sensitive/restricted data from the SDE system unless specified within their approved study plan by IRB and the data provider.
* The Researcher agrees not to attempt to circumvent or disable any of the security systems in place on the SDE system and to report to the CUIT-SDE Staff any attempts to circumvent or disable these systems that are known to him or her.
* The Researcher agrees to inform the CUIT-SDE staff of any change in their employment or University status.
* If the Researcher is primary investigator or co-investigator and the restricted data are subject to review by the Columbia University Institutional Review Board for Human Participants, he/she acknowledges that IRB approval will be maintained for the duration of the project.
* The Researcher acknowledges that the SDE Administrators may suspend or terminate access privileges at any time in order to protect the integrity of the confidential data.

The foregoing has been agreed to and accepted by the person(s) whose signature(s) appears below (Researchers).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Primary Investigator Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PI Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Research Staff Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Research Staff Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

**CUIT-SDE Data Security Officer (DSO) Agreement**

CUIT requires all SDE projects to designate one member as their Data Security Officer (DSO). DSOs are responsible for the uploading and downloading of project appropriate data and output files and enforcing the data security expectations associated with their project’s data agreement, IRB protocol data security specifications, and expectations outlined in this agreement. The DSO is required to sign the pledge of data confidentiality and protection below. As such, the undersigned employees and consultants of the SDE system agree to the following conditions:

1. Any and all IRB and Data Use Agreement security requirements will be monitored and enforced by the Data Security Officer (DSO). The DSO is responsible for failures in compliance by any and all members of their team.
2. The DSO staff member is authorized to access confidential data solely for the purpose of administering compliance with their project’s Data Use Agreement(s). They are not authorized to conduct research using the confidential data unless they are a researcher specified under the project’s IRB agreement..
3. The DSO staff member agrees that restricted data may not be placed on the SDE system nor removed from the system except as dictated by the terms of the Data Use Agreements between researchers and restricted data providers.
4. The DSO staff member with access to the SDE system agree not to allow anyone else to use their credentials to access the system.
5. The DSO staff member with access to the SDE system agree not to attempt to circumvent or disable any of the security systems in place on the SDE system.
6. When required by the researchers and approved by the Data Use Agreement, the DSO staff member agrees output files will be delivered to authorized users by a password protected and encrypted WinZip file via email or other methods considered appropriate under the IRB and Data Use Agreement security guideline to insure compliance.
7. This Agreement expires on *insert date*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data Security Officer Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data Security Officer Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date