Steps to Acquire and Use Restricted Data at Cornell

(Rev. 2/21/2013)

PROCESS FOR ACQUIRING AND ACCESSING DATA

1. Researcher meets with the CISER Secure Data Services Data Custodian to review procedures for access to restricted data, including but not limited to review of:
    a. Project description
    b. If researcher does not have PI status (for example, researcher is a graduate student or a Research Associate) then a PI eligible faculty member needs to be identified.
    c. Data provider's specific requirements
    d. Security plan requirements, both CISER's security plan and any data provider-specific security requirements
    e. Method of transmission of data to the Data Custodian
    f. Method and timing of disposal of data at end of project
    g. Affidavit of data security
2. Researcher communicates with data provider to clarify any questions (CISER available to assist with follow up on questions) and finalizes draft application
3. CISER reviews final draft of application for researcher
4. Researcher obtains IRB approval or exemption. Check the data provider's requirements for the time when the approval/exemption must be provided, as it can vary.
5. Researcher obtains departmental approval and submits Form 10 and complete application package to OSP
6. OSP reviews entire package for completeness and communicates with researcher about any missing items or questions.
7. OSP submits the application to the data provider for the researcher
8. OSP notifies the researcher and CISER when the agreement is fully executed and sends a copy of the approved Restricted Access Data Agreement to CISER.
9. Data provider transmits data to the CISER Data Custodian in the agreed manner
10. The CISER Data Custodian prepares the data for use, by
    a. copying the data to the secure CRADC server
    b. storing the original media in a safe in the CISER building
    c. if the original media are transmitted electronically and the data provider permits, CISER will copy the data to a physical media and store in a safe in the CISER building
11. Researcher signs a CISER computing use agreement specific to the terms of the data provider. This agreement is for one year and must be renewed annually.
12. CISER creates customized secure computing accounts
13. CISER provides users with training to enable them to use the secure data services efficiently and in accord with the requirements of the data provider.
14. IRB approval was required for the project then it must be renewed annually and is the researcher's responsibility. If the IRB approval expires then project user accounts will be suspended from the date of IRB expiration until IRB renewal has been granted.

PROCESS AT END OF APPROVAL PERIOD

15. Researcher notifies OSP and CISER when data use is complete, and/or if there is a need to extend the data use agreement. If there is a need to extend, notification should be sent at least 3 months before the existing termination date.

If Requesting an Extension:

16. Researcher's department submits a change request through the Portal with the required information for the extension request.
17. OSP requests approval from data provider to extend the use of data agreement.
18. Data provider provides OSP with Amendment for signature.
19. OSP receives fully executed Amendment from data provider and distributes to researcher, CISER, etc.

If Closing Out/Not Requesting an Extension:

20. Data provider submits to OSP the data providers required signed closeout documents (Affidavits) as required by the data provider.
21. CISER submits to data provider the required certification of destruction and/or return the data, as required by the data provider under the user agreement.