Restricted Data Use Agreement
for Restricted Data in the Virtual Data Enclave (VDE)
from the Inter-university Consortium
for Political and Social Research (ICPSR)

I. Definitions

A. "Investigator" is the person primarily responsible for conducting the research or statistical activities relative to the Research Description within the Online Application (the "Research Description"), or supervising the individuals conducting the research or statistical activities relative to the Research Description, for which Restricted Data are obtained through this Agreement.

B. "Research Staff" are all persons at the Investigator's Institution, excluding the Investigator, who will have access to Restricted Data obtained through this Agreement, including students, other faculty and researchers, staff, agents, or employees for which Institution accepts responsibility.

C. "Institution" is the university or research institution at which the Investigator will conduct research using Restricted Data obtained through this Agreement.

D. "Representative of the Institution" is a person authorized to enter into binding legal agreements on behalf of Investigator's Institution.

E. "Restricted Data" are the research dataset(s) provided under this Agreement that include potentially identifiable information in the form of indirect identifiers that if used together within the dataset(s) or linked to other dataset(s) could lead to the re-identification of a specific Private Person, as well as information provided by a Private Person under the expectation that the information would be kept confidential and would not lead to harm to the Private Person. Restricted Data includes any Derivatives.

F. "Private Person" means any individual (including an individual acting in an official capacity) and any private (i.e., non-government) partnership, corporation, association, organization, community, tribe, sovereign nation, or entity (or any combination thereof), including family, household, school, neighborhood, health service, or institution from which the Restricted Data arise or were derived, or which are related to a Private Person from which the Restricted Data arise or were derived.

G. "ICPSR" is the Inter-university Consortium for Political and Social Research.

H. "Online Application" includes all information entered into the ICPSR web-based data access request system, including Investigator information, Research Staff information, Research Description, Data Selection specifying which files and documentation are requested, Confidentiality Pledge signed by the Investigator, Supplemental Agreement and Confidentiality Pledge signed by each Research Staff, Data Security Plan, and a copy of a document signed by the Institution's Institutional Review Board (IRB), or equivalent, approving or exempting the research project.

I. “Data Security Plan” is a component of the Agreement which specifies permissible computer configurations for use of Restricted Data and records what the Investigator commits to do in order to keep Restricted Data secure.

J. “Deductive Disclosure” is the discerning of a Private Person's identity or confidential information through the use of characteristics about that Private Person in the Restricted Data. Disclosure risk is present if an unacceptably narrow estimation of a Private Person’s confidential information is possible or if determining the exact attributes of the Private Person is possible with a high level of confidence.

K. “Derivative” is a file or statistic derived from the Restricted Data that poses disclosure risk to any Private Person in the Restricted Data obtained through this Agreement. Derivatives include copies of the Restricted Data provided through ICPSR’s Virtual Data Enclave (VDE), subsets of the Restricted Data, and analysis results that do not conform to the guidelines in Section VI.F.

L. The “Virtual Data Enclave” permits monitored access to data that are not available to the general public. The virtual machine is isolated from the user's physical desktop computer, restricting the user from downloading files or parts of files to their physical computer. The virtual machine is also restricted in its external access, preventing users from emailing, copying, or otherwise moving files outside of the secure environment, either accidentally or intentionally.

II. Responsibility to Address Disclosure Risk

Deductive Disclosure of a Private Person's identity from research data is a major concern of federal agencies, researchers, and Institutional Review Boards. Investigators and Institutions who receive any portion of Restricted Data are obligated to protect the Restricted Data from Deductive Disclosure risk, non-authorized use, and attempts to identify any Private Person by strictly adhering to the obligations set forth in this Agreement.

III. Requirements of Investigator

A. The Investigator assumes the responsibility of completing the Online Application and any other required documents, reports, and amendments.

B. The Investigator agrees to manage and use Restricted Data, implement all Restricted Data security procedures per the Data Security Plan, and ensure that all Research Staff understand their requirements per this Agreement and follow the Data Security Plan.

C. Investigators must meet each of the following criteria:

1. Have a PhD or other research-appropriate terminal degree; and
2. Hold a faculty appointment or have an appointment that is eligible to be a principal investigator at Institution.

IV. Requirements of Institution

The Institution represents that it is:

A. An institution of higher education, a research organization, a research arm of a government agency, or a nongovernmental, not-for-profit, agency.

B. Not currently debarred or otherwise restricted in any manner from receiving information of a sensitive, confidential, or private nature under any applicable laws, regulations, or policies.

C. Have a demonstrated record of using sensitive data according to commonly accepted standards of research ethics and applicable statutory requirements.

V. Obligations of ICPSR

In consideration of the promises made in Section VI of this Agreement, and upon receipt of a complete and approved Online Application, ICPSR agrees to:

A. Provide the Restricted Data requested by the Investigator in the Restricted Data Order Summary within a reasonable time of execution of this Agreement by Institution and to make the Restricted Data available to Investigator via the Virtual Data Enclave, a secure remote-access work space. Access requires proper authentication. ICPSR will provide instructions on establishing user accounts within a reasonable amount of time after the execution of the agreement.

B. Provide electronic documentation of the origins, form, and general content of the Restricted Data sent to the Investigator, in the same time period and manner as the Restricted Data.

ICPSR MAKES NO REPRESENTATIONS NOR EXTENDS ANY WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED. THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE USE OF THE RESTRICTED DATA WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS. Unless prohibited by law, Institution assumes all liability for claims for damages against them by third parties that may arise from the use, storage, disposal, or disclosure by the Institution of the Restricted Data, except to the extent and in proportion such liability or damages arise from the negligence of ICPSR.

VI. Obligations of the Investigator, Research Staff, and Institution

Restricted Data access provided under this Agreement shall be used or disclosed only in compliance with the terms of this Agreement. In consideration of the promises in Section V of this Agreement, and for use of Restricted Data from ICPSR, the Institution agrees:

A. That the Restricted Data will be used solely for research or statistical purposes relative to the project as identified in the Research Description of the Online Application (the “Research Description”), and for no other purpose whatsoever without the prior written consent of ICPSR. Further, no attempt will be made to identify Private Person(s), no Restricted Data of Private Person(s) will be published or otherwise distributed, the Restricted Data will be protected against Deductive Disclosure risk by strictly adhering to the obligations set forth in this Agreement, and precautions will be taken to protect the Restricted Data from non-authorized use.

B. To comply fully with the approved Data Security Plan at all times relevant to this Agreement.

C. That no persons other than those identified in this Agreement or in subsequent amendments to this Agreement, as Investigator or Research Staff and who have signed this Agreement or a Supplemental Agreement, be permitted access to the contents of Restricted Data files or any Derivatives from the Restricted Data.

D. That within five (5) business days of becoming aware of any unauthorized access, use, or disclosure of Restricted Data, or access, use, or disclosure of Restricted Data that is inconsistent with the terms and conditions of this Agreement, the unauthorized or inconsistent access, use, or disclosure of Restricted Data will be reported in writing to ICPSR.

E. That, unless prior specific, written approval is received from ICPSR, no attempt under any circumstances will be made to link the Restricted Data to any Private Person, whether living or deceased, or with any other dataset, including other datasets provided by ICPSR.

F. To avoid inadvertent disclosure of Private Persons by being knowledgeable about what factors constitute disclosure risk and by using disclosure risk guidelines, such as but not limited to, the following guidelines[1] in the release of statistics or other content derived from the Restricted Data.[2]

1. No release of a sample unique for which only one record in the Restricted Data provides a certain combination of values from key variables.
2. No release of a sample rare for which only a small number of records (e.g., 3, 5, or 10 depending on sample characteristics) in the Restricted Data provide a certain combination of values from key variables. For example, in no instance should the cell frequency of a cross-tabulation, a total for a row or column of a cross-tabulation, or a quantity figure be fewer than the appropriate threshold as determined from the sample characteristics. In general, assess empty cells and full cells for disclosure risk stemming from sampled records of a defined group reporting the same characteristics.
3. No release of the statistic if the total, mean, or average is based on fewer cases than the appropriate threshold as determined from the sample characteristics.
4. No release of the statistic if the contribution of a few observations dominates the estimate of a particular cell. For example, in no instance should the quantity figures be released if one case contributes more than 60 percent of the quantity amount.
5. No release of data that permits disclosure when used in combination with other known data. For example, unique values or counts below the appropriate threshold for key variables in the Restricted Data that are continuous and link to other data from ICPSR or elsewhere.

---

[1] For more information, see the National Center for Health Statistics checklist, *NCHS Disclosure Potential Checklist* at http:// http://www.cdc.gov/nchs/data/nchs_microdata_release_policy_4-02A.pdf; and *FCSM Statistical Policy Working Paper 22 (Second Version, 2005)* at http://www.hhs.gov/sites/default/files/spwp22.pdf

[2] If disclosure review rules were established for a specific Restricted Dataset, they will be included in the dataset's documentation and are covered by this Agreement.

6. No release of minimum and maximum values of identifiable characteristics (e.g., income, age, household size, etc.) or reporting of values in the "tails," e.g., the 5^{th} or 95^{th} percentile, from a variable(s) representing highly skewed populations.
7. No release of ANOVAs and regression equations when the analytic model that includes categorical covariates is saturated or nearly saturated. In general, variables in analytic models should conform to disclosure rules for descriptive statistics (e.g., see #6 above).
8. In no instance should data on an identifiable case, or any of the kinds of data listed in preceding items 1-7, be derivable through subtraction or other calculation from the combination of tables released.
9. No release of sample population information or characteristics in greater detail than released or published by the researchers who collected the Restricted Data. This includes but is not limited to publication of maps.
10. No release of anecdotal information about a specific Private Person(s) or case study without prior written approval.
11. The above guidelines also apply to charts as they are graphical representations of cross-tabulations. In addition, graphical outputs (e.g., scatterplots, box plots, plots of residuals) should adhere to the above guidelines.

G. That if the identity of any Private Person should be discovered, then:
   1. No use will be made of this knowledge;
   2. ICPSR will be advised of the incident within five (5) business days of discovery of the incident;
   3. The information that would identify the Private Person will be safeguarded or destroyed as requested by ICPSR; and
   4. No one else will be informed of the discovered identity.

H. Unless other provisions have been made with ICPSR, all access to the Restricted Data will be terminated on or before completion of this Agreement or within five (5) days of written notice from ICPSR. Investigators requiring access to the Restricted Data beyond completion of this Agreement should submit a request for continuation three months prior to the end date of the Agreement.

I. That any books, articles, conference papers, theses, dissertations, reports, or other publications that employed the Restricted Data or other resources provided by ICPSR reference the bibliographic citation provided by ICPSR and be reported to ICPSR for inclusion in its data-related bibliography.

J. To provide annual reports to ICPSR staff (through ICPSR's online data access request system), which include:
   1. A copy of the annual IRB approval for the project described in the Research Description;
   2. A listing of public presentations at professional meetings using results based on the Restricted Data or Derivatives or analyses thereof;

3. A listing of papers accepted for publication using the Restricted Data, or Derivatives or analyses thereof, with complete citations;
4. A listing of Research Staff using the Restricted Data, or Derivatives or analyses thereof, for dissertations or theses, the titles of these papers, and the date of completion; and
5. Update on any change in scope of the project as described in the Research Description.

K. To notify ICPSR of a change in institutional affiliation of the Investigator, a change in institutional affiliation of any Research Staff, or the addition or removal of Research Staff on the research project. Notification must be in writing and must be received by ICPSR at least six (6) weeks prior to the last day of employment with Institution. Notification of the addition or removal of Research Staff on the research project shall be provided to ICPSR as soon as reasonably possible. Investigator's separation from Institution terminates this Agreement.

L. Investigator may reapply for access to Restricted Data as an employee of the new institution. Re-application requires:
1. Execution of a new Agreement for the Use of Restricted Data by both the Investigator and the proposed new institution;
2. Execution of any Pledges of Confidentiality by Research Staff at the proposed new institution;
3. Preparation and approval of a new Data Security Plan; and
4. Evidence of approval or exemption by the proposed new institution's IRB.

These materials must be approved by ICPSR before Restricted Data or any derivatives or analyses may be accessed at the new institution.

M. That if the Investigator who is changing institutions does not have the new agreement executed by the time they leave their institution, ICPSR will temporarily deactivate the Investigator's account but will maintain the Investigator's profile to save their work during the transition. Upon approval of the new online application, ICPSR will reactivate the Investigator's account. If a new agreement is not executed within three (3) month, the Investigator's account will be deleted.

N. That use of the Restricted Data will be consistent with the Institution's policies regarding scientific integrity and human subjects research.

O. To respond fully and in writing within ten (10) working days after receipt of any written inquiry from ICPSR regarding compliance with this Agreement.

VII. Violations of this Agreement

A. The Institution will investigate allegations by ICPSR or other parties of violations of this Agreement in accordance with its policies and procedures on scientific integrity and misconduct. If the allegations are confirmed, the Institution will treat the violations as it would violations of the explicit terms of its policies on scientific integrity and misconduct.

B. In the event of a breach of any provision of this Agreement, Institution shall be responsible to promptly cure the breach and mitigate any damages. The Institution hereby acknowledges that any breach of the confidentiality provisions herein may result in irreparable harm to ICPSR not adequately compensable by money damages. Institution hereby acknowledges the possibility of injunctive relief in the event of breach, in addition to money damages. In addition, ICPSR may:

   1. Terminate this Agreement upon notice and immediately remove access to Restricted Data and any derivatives thereof;
   2. Deny Investigator future access to Restricted Data; and/or
   3. Report the inappropriate use or disclosure to the appropriate federal and private agencies or foundations that fund scientific and public policy research.
   4. Such other remedies that may be available to ICPSR under law or equity, including injunctive relief.

C. Institution agrees, to the extent not prohibited under applicable law, to indemnify the Regents of the University of Michigan from any or all claims, losses, causes of action, judgments, damages, and expenses arising from Investigator's, Research Staff's, and/or Institution's use of the Restricted Data, except to the extent and in proportion such liability or damages arose from the negligence of the Regents of the University of Michigan. Nothing herein shall be construed as a waiver of any immunities and protections available to Institution under applicable law.

D. In the event of a violation, the Investigator must:
   1. Notify ICPSR within five (5) business days;
   2. Stop work with the Restricted Data immediately;
   3. Submit a notarized affidavit acknowledging the violation to ICPSR;
   4. Inform the Representative of Institution of the violation and review security protocols and disclosure protections with them.
      i. The Representative of Investigator's Institution must submit an acknowledgment of the violation and security protocols and disclosure protections review to ICPSR; and
   5. Reapply for access to the Restricted Data.

VIII. Confidentiality

To the extent the Restricted Data are subject to a Certificate of Confidentiality, the Institution is considered to be a contractor or cooperating agency of ICPSR; as such, the Institution, the Investigator, and Research Staff are authorized to protect the privacy of the individuals who are the subjects of the Restricted Data by withholding their identifying characteristics from all persons not connected with the conduct of the Investigator's research project. "Identifying characteristics" are considered to include those data defined as confidential under the terms of this Agreement.

IX. Incorporation by Reference

All parties agree that the information entered into the Online Application, including the Data Security Plan, IRB approval, and any Supplemental Agreements and Confidentiality Pledges, are incorporated into this Agreement by reference.

X. Miscellaneous

A. All notices, contractual correspondence, and return of Restricted Data under this Agreement on behalf of the Investigator shall be made in writing and delivered to the address below:

   ICPSR
   P.O. Box 1248
   Ann Arbor, MI 48106-1248
   -or-
   help@icpsr.umich.edu

B. This agreement shall be effective for 24 months from execution or until the IRB expires, whichever occurs first.

C. The respective rights and obligations of ICPSR and Investigator, Research Staff, and Institution pursuant to this Agreement shall survive termination of the Agreement.

D. This Agreement and any of the information and materials entered into the Online Application may be amended or modified only by the mutual written consent of the authorized representatives of ICPSR and Investigator and Institution. Both parties agree to amend this Agreement to the extent necessary to comply with the requirements of any applicable regulatory authority.

E. The Representative of the Institution signing this Agreement has the right and authority to execute this Agreement, and no further approvals are necessary to create a binding agreement.

F. The obligations of Investigator, Research Staff, and Institution set forth within this Agreement may not be assigned or otherwise transferred without the express written consent of ICPSR.

Investigator and Institutional Signatures

Read and Acknowledged by:

Investigator	**Institutional Representative**
SIGNATURE DATE	SIGNATURE DATE
NAME TYPED OR PRINTED	NAME TYPED OR PRINTED
TITLE	TITLE
INSTITUTION	INSTITUTION
BUILDING ADDRESS	BUILDING ADDRESS
STREET ADDRESS	STREET ADDRESS
CITY, STATE ZIP	CITY, STATE ZIP

Attachment A: Data Security Plan

All of the following computer and data security requirements and procedures are required to be implemented as part of this Agreement:

- You must password protect the computer that is used to access the Confidential Data.
- Under no circumstances may you share or give your VDE username and password to anyone, and this includes not sharing them with other members of your project team or your organization's IT staff. Passwords must not be stored on a computer in electronic or written form. Software password storage programs may not be used.
- Since the Confidential Data are administered by ICPSR, University of Michigan you should not contact the IT staff at your organization with questions about the Confidential Data. (You may contact your organization's IT staff if you need help installing the VM client software to access the Confidential Data. Your organization's IT staff should never be allowed to access any Confidential Data.)
- Under no circumstances can any unauthorized person be allowed to access or view Confidential Data within the VDE.
- Unauthorized persons are not allowed to be inside the Secure Project Office when an authorized project team member is logged into the VDE.
- You must not allow the computer monitor to display Confidential Data content to any unauthorized person. The computer monitor display screen must not be visible from open doors or through windows.
- You must set the computer to activate a password protected screen saver after three minutes of inactivity.
- If you are logged into the VDE and you leave your computer,you must "disconnect" or "logoff" from the VDE. (Disconnecting from the VDE will leave any open programs running, but closes the connection to the VDE. Logging off of the VDE closes the connection and terminates all programs that are running.)
- All Confidential Data must be kept within the VDE:
    - o You must not duplicate or copy the data (e.g., you must not retype and/or use non-technical ways of copying the data, such as handwritten notes).
    - o You must not take screenshots, photographs, or videos of the displayed Confidential Data or statistical outputs.
    - o You must not type or record the Confidential Data or results from the data onto your PC or onto some other device or media.
- You must protect all hardcopy documents related to the Confidential Data such as research notes. Such hardcopy documents must be kept in locked drawers or cabinets when not in use.
- Prior to a disclosure review and approval by ICPSR, neither you nor any project team member may talk about or discuss any Confidential Data or results from the VDE in non-secure or public locations. These discussions cannot occur where an unauthorized person could eavesdrop.
- You must submit all statistical outputs/results from the VDE to ICPSR for a disclosure review prior to sharing or giving such outputs to unauthorized persons. You also agree to revise or alter such outputs as required by ICPSR in orderto minimize disclosure risk prior to ICPSR approving these outputs for dissemination to unauthorized persons.
- You may only disseminate aggregated information from the Confidential Data to unauthorized persons after you obtain clearance to do so through the ICPSR disclosure review process.
- Each member of your research team included in this application must only use the

data on a computer in a Secure Project Office.