MiCDA Affiliate Initial Application
to use the MiCDA Virtual Data Enclave (VDE)

Checklist

- ☐ **I. Affiliate Information**
- ☐ **II. Project Information**
- ☐ **III. Data Use Agreement Information**
- ☐ **IV. List of users requesting VDE access**
- ☐ **V. Forms to be completed by <u>each user</u> requesting MiCDA VDE access**
  - ☐ Signed Acceptable Use Policy (AUP)
  - ☐ Signed Institute for Social Research Pledge to Safeguard Respondent Privacy
  - ☐ Signed Data Security Plan
- ☐ **VI. Additional Required Attachments**
  - ☐ Copy of Fully Executed Data Use Agreement(s)
  - ☐ Copy of IRB approval(s)

Send all materials to MiCDAEnclave@umich.edu.

MiCDA Affiliate Initial Application
to use the MiCDA Virtual Data Enclave (VDE)

I. Affiliate Information

_____ _____

First Name Last Name

_____

Title

_____

Department

_____

School/Unit at the University of Michigan

II. Project Information

Project Title: _____

Brief Abstract (200-250 words recommended):

Project Funder/Grant Number (if applicable): _____

☐ Check if interested in discussing high performance computing options with MiCDA Staff.

III. Data Use Agreement Information

Please list the Data Provider on the Data Use Agreement

_____
Data Provider

Please specify project's designated disclosure reviewer. (Typically, this is the PI or designated project staff person.)

Reviewer: _____ Email: _____

Please summarize disclosure review requirements as indicated in the Data Use Agreement with the Data Provider.

Rule	Description	MiCDA Default Values	Indicate Alternative from Your Data Use Agreement if Specified
Personally Identifiable Information	Names, addresses and other identifiers	May not be removed	
List of cases or microdata	Individual cases listed or in a data set	May not be removed	
Geographic visualizations	Maps	May not be removed	
Minimum cell sizes	For tables, minimum allowed cell sizes. Cells below this value require rows or columns to be combined (suppressing cell < 11 is not adequate).	11	
Suppressed Variables	These variables can be included in analysis, but cannot be used as stratifiers or selection variables in tables and coefficients cannot be reported	Geography at state or lower level	
Other, specify	--	--	

MiCDA Affiliate Initial Application
to use the MiCDA Virtual Data Enclave (VDE)

IV. List of users requesting VDE Access

Please list all users who will require access to the VDE to work on the project. Copy this sheet to add more collaborators. All collaborators must be listed on the data use agreement. All collaborators must have IRB approval (or proof that another institution serves as the IRB of record).

User #1 (Begin with Applicant)

_____ _____
First Name Last Name

_____
Title

_____
Department

_____
Institution

User #2

_____ _____
First Name Last Name

_____
Title

_____
Department

_____
Institution

User #3

_____ _____
First Name Last Name

_____
Title

_____
Department

_____
Institution

User #4

_____ _____
First Name Last Name

_____
Title

_____
Department

_____
Institution

User #5

_____ _____
First Name Last Name

_____
Title

_____
Department

_____
Institution

User #6

_____ _____
First Name Last Name

_____
Title

_____
Department

_____
Institution

V. Forms to be completed by <u>each user</u> requesting MiCDA VDE access

MiCDA Secure Data Enclave
Acceptable Use Policy (AUP)

1. I understand that I have the primary responsibility to safeguard the information contained in the MiCDA Secure Data Enclave (SDE) from unauthorized use, disclosure, inadvertent modification, destruction, or denial of service.

2. Access to the SDE is for authorized purposes only. Access to these resources is a revocable privilege and is subject to content monitoring and security testing.

3. I will only use equipment approved by the sponsoring project to access the SDE.

4. I will only access the SDE from the location approved by the sponsoring project.

5. I will position my computer screen to prevent unauthorized user from viewing SDE data. I will lock my computer if I step away from it.

6. I will use approved data transfer procedures for uploading or downloading information from any system or storage media. I will not introduce unauthorized software.

7. I will not print or reproduce SDE data.

8. If I observe anything on the SDE (or system that I use to access it) which indicates inadequate security, then I will immediately notify my Enclave representative.

9. The following activities are specifically prohibited by any user on the MiCDA SDE:

9.1. Use of information systems for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes.

9.2. Attempts to strain, test, circumvent, or bypass network or SDE security mechanisms, or to perform network or keystroke monitoring.

9.3. Disabling or removing security or protective software and other mechanisms and their associated logs from the SDE.

9.4. Modification of the SDE, software installed therein, use of it in any manner other than its intended purpose, or adding user-configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications.

9.5. Installation of software, changing configuration of the SDE, or connecting the SDE to an unauthorized computer.

9.6. Sharing personal accounts and authenticators (passwords and/or token values) or permitting the use of remote access capabilities to any unauthorized individual.

9.7. Taking screenshots, pictures, screen-sharing, transcribing or otherwise duplicating images of any Enclave systems or their interfaces. This includes data, whether original or derived, and the results of data analysis.

10. I acknowledge and consent to the following conditions when I access the MiCDA SDE:

10.1. The Survey Research Center (SRC) routinely intercepts and monitors communications on the Enclave for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, and personnel misconduct investigations.

10.2. SRC may inspect, and if necessary remove, data stored on the SDE.

10.3. Data stored on the Enclave are not private, are subject to routine monitoring and inspection, and may be disclosed to the sponsoring project, my employer, and any regulating bodies.

10.4. The SDE includes security measures (e.g., authentication and access controls) to protect the sensitive data stored within--not for my personal benefit or privacy.

11. I will immediately report suspicious system activity or concerns to my SDE representative.

By signing this user agreement, I am acknowledging that I accept and will abide by all the terms and conditions described above.

_____ _____

Signature Date

_____

Printed Name

Institute for Social Research
University of Michigan

PLEDGE TO SAFEGUARD RESPONDENT CONFIDENTIALITY

I have read the Institute for Social Research Policy on Safeguarding Respondent Confidentiality, and pledge that I will strictly comply with that Policy. Specifically:

I will not reveal the name, address, telephone number, or other identifying information of any respondent (or family member of a respondent or other informant) to any person other than an employee directly connected to the study in which the respondent is participating.

I will not reveal the contents or substance of the responses of any identifiable respondent or informant to any person other than an employee directly connected to the study in which the respondent is participating, except as authorized by the project director or authorized designate.

I will not contact any respondent (or family member, employer, other person connected to a respondent or informant) except as authorized by the project director or authorized designate.

I will not release a dataset (including for unrestricted public use or for other unrestricted uses) except in accordance with authorization, policies and/or procedures established by ISR and the Center with which I am affiliated.

I will take all necessary precautions to avoid unintended disclosure of confidential information, including securing of paper and electronic records, computers, user IDs and passwords.

I agree that compliance with this Pledge and the underlying Policy is: 1) a condition of my employment (if I am an employee of ISR), and/or 2) a condition of continuing collaboration and association with ISR (if I am an affiliate of ISR). I understand that violation of this Policy and Pledge may result in disciplinary action, up to and including termination of employment or severance of any relationship with ISR and the applicable research project.

If I supervise affiliates who have access to ISR respondent data (other than unrestricted public release datasets), I will ensure that those affiliates adhere to the same standards of protection of ISR respondent privacy, anonymity, and confidentiality, as required by this Pledge and the associated Policy.

Signature: _____

Typed or printed name: _____ Date: _____

Affiliation (if non-ISR employee): _____

MICDA Enclave Virtual Desktop Infrastructure (VDI) Data Security Plan

Complete ONE Form for EACH User and EACH User Location

Work Location: From where will you log in? CHOOSE ONE:

Home: ☐ Address: Work: ☐ (Work address should include office #, bldg name, street address, city, state, and zip)

Workstation Specifications:

Make/model: _____

Form Factor: Desktop ☐ Laptop ☐

Operating System (Please note version #): Windows: ☐ Version: _____

Mac: ☐ Version: _____

Workstation Login Access: Who can log into your workstation?

Yourself: ☐ Other(specify):_____

What information is required at login on your computer?

User name: Yes ☐ No ☐ Password: Yes ☐ No ☐

Workstation Monitor Position: Describe how workstation is positioned to prevent unauthorized viewing (check windows and doors. If monitor is in an open or shared space it needs a screen filter):

Workstation Antivirus: Describe **brand and version** of antivirus software installed on workstation:

☐ Windows Defender ☐ Symantec ☐ McAfee

☐ Sophos ☐ Norton Version:_____

Other(specify brand/version:_____

Data Resource(s) Requested (select all that apply):

☐ HRS ☐ PSID ☐ NHATS

☐ Other(specify):_____

Smartphone Number: Download of DUO Mobile application is required for Two-Factor Authentication

Use of a smartphone is the simplest, fastest, and most cost-effective method for two-factor authentication. If this is not possible, a standard cellular phone or landline may be used, but expect delays and potential future costs associated with these methods.

Investigator Name Contract/Project #, if known

User Name User Title User Institution

User Signature Date User Email

Provide signature of an IT Representative familiar with the workstation described. ***Required unless it is a personally owned machine used in a home office OR the current work environment does not permit in-person contact with the IT representative.**

IT Department Contact Name IT Contact Title IT Contact Telephone

IT Contact Signature Date IT Contact Email

VI. Additional Required Attachments

Please attach a copy of your Fully Executed Data Use Agreement(s) with the Data Provider(s) and a copy of all IRB approval(s).