

**Research Computing Environment:**

- **Physical Enclave:** You will visit the Enclave facility housed in the Institute for Social Research, Ann Arbor, MI. **You do not need to complete this form.**
- **Virtual Desktop Infrastructure (VDI):** You will access data from your home institution, using a somewhat streamlined application. **Preferred solution.** [Go to page 2]
- **Standalone Workstation:** You plan to use HRS restricted data on a computer/workstation that is **physically isolated (air gap)** from the outside world. Recommended solution. [Go to page 3]

*If your computing environment does not fall into one of the above categories, please contact [HRSRDAApplication@umich.edu](mailto:HRSRDAApplication@umich.edu) for next steps.*

**Work site requirement:** We require that the work environment of HRS Restricted Data users be a secure office or work space owned by the signing institution. If the workspace is shared, then all occupants must sign the Restricted Data Agreement.

# MICDA Enclave Virtual Desktop Infrastructure (VDI) Data Security Plan

Complete ONE Form for EACH User and EACH User Location

**VDI requires an operating system of Windows 7 or higher.**

<b>Work Location</b>	Where will you login from? (street address, building, office number, city, state, zip)
<b>Workstation Specifications</b>	Tell us about your computer. Please describe make/model, form factor, Windows Operating System version:
<b>Work Station Access</b>	Explain who has workstation login access and please describe access controls in detail:
<b>Workstation Monitor</b>	Describe how workstation monitor is positioned to prevent unauthorized viewing:
<b>Workstation Anti-Virus</b>	Describe brand and version of anti-virus software installed on the workstation:
<b>Data Resource(s) Requested</b>	(check all that apply)  <div style="display: flex; justify-content: space-around;"> <span>Health and Retirement Study Monitoring the Future</span> <span>Panel Study of Income Dynamics</span> </div> Other (Specify):
<b>Smartphone Number for Two-Factor Authentication</b>	Please provide your Smartphone telephone number _____  <b>Download of DUO Mobile app is required.</b>
<i>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 - please expect some delays and potential future costs associated with these methods.</i>	

Investigator Name	Title	Institution
-------------------	-------	-------------

Investigator Signature	Date	Resource Reference #, if known
------------------------	------	--------------------------------

**Complete the following for Institutional Settings Only**

IT Department Contact Name	Title	Telephone
----------------------------	-------	-----------

IT Contact Signature	Date	
----------------------	------	--

## Standalone Workstation (Physically Isolated with Air Gap)

<b>Workstation Location</b> (Street address, Building, Office number)	
<b>Operating System</b> (check one)	<input type="radio"/> Windows 7 Professional/Enterprise/Ultimate <input type="radio"/> Macintosh OS X (10.4 and above) <input type="radio"/> Unix family (specify) <input type="radio"/> Other (specify)
<b>Workstation Specifications</b>	<b>Please describe (make/model, form factor):</b>
<b>Network Connections</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Are all external network connections to the workstation disabled?</b> If the answer to this question is NO, please contact <a href="mailto:HRSRDAAApplication@umich.edu">HRSRDAAApplication@umich.edu</a> for assistance.
<b>Laptop</b> <input type="radio"/> Yes* <input type="radio"/> No	<b>Will a laptop be used as the workstation?</b> If yes, provide research justification (this solution is strongly discouraged). You should also explain in detail how wireless connectivity will be disabled. Use the space provided at the end of this section.
<b>Workstation Login Access</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is workstation login access limited to person(s) specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i>?</b>
<b>Workstation Location Access</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is the workstation stored in locked office accessible only to the persons specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i>?</b>
<b>Workstation Monitor</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is the workstation monitor positioned to prevent unauthorized viewing?</b>
<b>Workstation Protection</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is physical protection provided for workstation hardware (e.g., BIOS password, locked CPU box)?</b> Describe:
<b>Workstation Removable Media</b> <input type="radio"/> Yes* <input type="radio"/> No	<b>Will removable media be used for storage of restricted data? If yes,</b> in the space provided at the end of this section state: (1) where the removable media to be used will be physically located, (2) how physical access to them is to be restricted and (3) how access to the contents will be controlled.
<b>Workstation Secure Updates</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is a procedure in place to allow secure updating of workstation operating system and applications software?</b> Describe:
<b>Workstation Anti-Virus</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is anti-virus software installed on the workstation?</b> Describe:

<b>Encryption Installed</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Is strong encryption (e.g., Bitlocker, Windows Encrypting File System, PGP) installed and in use on the workstation?</b> Describe:
<b>Encryption Usage</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Are restricted data files kept in encrypted form when not in use?</b> Describe:
<b>Backups</b> <input type="radio"/> Yes* <input type="radio"/> No	<b>Will backups be performed on restricted data files stored on this workstation?</b> If yes, describe the physical and/or software methods to be used.
<b>Original Media Storage</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Will restricted data media received from HRS be stored in a secure location?</b>
<b>Printed Output</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>Are procedures in use to minimize the printing of restricted data elements?</b>
<b>Printer Location</b> <input type="radio"/> Yes <input type="radio"/> No*	<b>If a local printer is used for printed output is it located in the same locked office as the standalone workstation?</b>

**Use this space for explanatory information concerning starred (\*) items:**

Investigator Name	Title	Institution
IT Department Contact Name	Title	Telephone
IT Contact Signature	Date	HRS RDA #, if known