

MICDA Enclave Virtual Desktop Infrastructure (VDI) Data Security Plan
Complete ONE Form for EACH User and EACH User Location
See next page for descriptions of each field

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	
Other(specify): _____			
Smartphone Number: Download of DUO Mobile application is required for Two-Factor Authentication			
<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, but expect delays and potential future costs associated with these methods.</i>			

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**

IT Department Contact Name

IT Contact Title

IT Contact Telephone

IT Contact Signature

Date

IT Contact Email

Work Location

This may be a home office, or Institutional workspace. It must be a designated, consistent location. Private offices are preferred. If a user is working in a shared office, or a cubicle, or other shared workspace, a privacy screen is required. If an Institutional space, an office number must be designated.

Workstation Specifications

The MiCDA SDE can be accessed from both Windows and Mac computers. User must designate the make/model (i.e. HP Z420), form factor (i.e. desktop, laptop), and operating system with version number (i.e. Mac OSX Mojave 10.14.13). Any computer may be used, but the operating system must be one that is currently supported by the software maker.

Workstation Login Access

Users must designate who can login, and how that is controlled. Login access is typically controlled via username and password. Whether this a local only account or centrally provisioned and controlled account should be noted. If more individuals than the HRS user can login, access to user files must be restricted by user account. This must be noted on the DSP.

Workstation Monitor Position

Monitor(s) must be positioned to prevent viewing by unauthorized individuals. Users should describe how their monitor(s) is/are positioned in their workspace in relation to windows and doors. If a user is working in a shared office, or a cubicle, or other shared workspace, a privacy screen is required.

Workstation Antivirus

An actively updated antivirus application must be installed. The only products currently forbidden for use with systems accessing the MiCDA are Kaspersky and 360 Labs. Most other antivirus products will be approved. HRS reserves the right to deny use of an antivirus at the project's discretion.