



MiCDA Enclave Virtual Desktop Infrastructure Data Security Plan

Complete ONE Form for EACH User and EACH User Location

Work Location: Where will you log in? CHOOSE ONE: ☐ Home ☐ Office*		
Address (*Office address should include office #, building name, street address, city, state, and zip)		
<u>Note: NHATS data in the MiCDA enclave may not be accessed by persons located in "countries of concern" as identified pursuant to 28 CFR Part 202.</u>		
Do you have a private or shared office? ☐ Private ☐ Shared		
Workstation ownership: Who owns your workstation (computer)?		
☐ Your Institution ☐ Yourself (personally-owned)		
Workstation Specifications: ☐ Desktop ☐ Laptop		
Make/model: _____		
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 your workstation is positioned to prevent unauthorized viewing (check windows and doors):		
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): ☒ NHATS		
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		
User Name	NHATS User Name	User Institution
User Signature	Date	User Email

NHATS Data Protection Plan Requirements

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, then a privacy screen is required. If working from 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. macOS 26.0.1 Tahoe). Any computer may be used, but the operating system must be one that is currently supported by the software maker. As of October 14th 2025, Windows 10 is no longer supported by Microsoft with security updates unless you are running Windows 10 with Extended Security Updates (ESUs), or Windows 10 LTSC. Windows 11 home edition is also not allowed.

How to Get System Information

Click the Windows icon on the bottom left of your screen and then type "System Information". In the window that pops up after you select system information, there are two fields, system manufacturer (Make), and System Model (Model). This window will also show you your OS, and OS version.

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 just the designated 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. Describe how the monitors are positioned in relation to doors and windows in the Workstation Monitor Position section of the form. 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. NHATS reserves the right to deny use of an antivirus at our discretion.