MICDA/SRC 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 monitor is positioned ***in relation to windows and doors in room*** to prevent unauthorized viewing. 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:____________________

Server (For administration use only}:

MiCDA: □ □ HRS □ PSID □ NHATS SRC: □ □ MTF □ PSC □ CPS □ PSID

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

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 11 or 12). 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 PSID 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 anti virus application must be installed. The only products currently forbidden for use with systems accessing the MiCDA are Kaspersky and 360 Labs. Most other anti virus products will be approved. PSID reserves the right to deny use of an anti virus at the project's discretion.

End-user device operating systems and anti-virus software for use with the SDI

Windows

Approved: Windows 8.1
Windows 10
Windows 11

NOTE: As of January, 2020 all end users must be running Windows 8.1 or (preferably) Windows 10 as Win 7 is no longer supported by Microsoft.

Anti-virus: Currently, only Kaspersky and 360 antivirus applications are prohibited for use on computers connecting to the enclave.

Mac OSX

Approved: 11 Big Sur
12 Monterey

NOTE - As of NOV. 2021, OSX 10.14 (Mojave) is officially no longer supported. Apple released the final security update for 10.15 (Catalina) at this time as well. Since 10.15 will not be receiving updates, ISR considers it unsupported. Users must use the most recent version of Microsoft RDP to connect to the SDI VDI systems.

Anti-virus: Mac OSX does not have a built-in anti-virus program. A third-party anti-virus program is needed. There are many anti-virus programs available for the Mac OS (see www.macworld.com and search for antivirus for options). If your computer is owned by your workplace, it is best to install their recommended anti-virus software. If they do not have a recommendation, frequently used antivirus programs include Sophos, Bit Defender, and Trend Micro.

Linux

Approved: None

Linux does not have a Remote Desktop Protocol application capable of handling Terminal Services Gateway connections. This is a requirement of the SDI VDI systems.

UPDATED: 11/10/2021