# MiCDA Sensitive Data Enclave
# Acceptable Use Policy (AUP)

**1.** I understand that I have the primary responsibility to safeguard the information contained in the MiCDA Sensitive 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.

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

**6.** I will not print or reproduce SDE data.

**7.** 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.

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

> **8.1.** 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.
>
> **8.2.** Attempts to strain, test, circumvent, or bypass network or SDE security mechanisms, or to perform network or keystroke monitoring.
>
> **8.3.** Disabling or removing security or protective software and other mechanisms and their associated logs from the SDE.
>
> **8.4.** 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.
>
> **8.5.** Installation of software, changing configuration of the SDE, or connecting the SDE to an unauthorized computer.

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

**8.7** Taking screenshots, pictures, or otherwise duplicating images of any Enclave systems or their interfaces. This includes data, whether original or derived, and the results of data analysis.

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

**9.1.** The 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.

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

**9.3.** 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.

**9.4.** 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.

**10.** 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