CJARS Virtual Data Enclave
Acceptable Use Policy

1. I understand that I have the primary responsibility to safeguard CJARS Virtual Data Enclave (VDE) information from unauthorized use, disclosure, inadvertent modification, destruction, or denial of service.

2. Access to the CJARS VDE 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 listed in my Data Security Plan to access the CJARS VDE.

4. I will only access the CJARS VDE from the location(s) listed in my Data Security Plan.

5. I will position my computer screen to prevent unauthorized users from viewing CJARS VDE data. I will lock my computer if I step away from it.

6. I will not remove, or attempt to remove, any data or statistical output from the CJARS VDE before receiving explicit disclosure approval. I will not introduce, or attempt to introduce, unauthorized software.

7. I will not print or reproduce CJARS VDE data.

8. If I observe anything on the CJARS VDE (or system that I use to access it) which indicates inadequate security, then I will immediately notify a CJARS VDE representative by emailing cjars-vde-users@umich.edu.

9. The following activities are specifically prohibited by any user on the CJARS VDE:

    a. 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.

    b. Attempts to strain, test, circumvent, or bypass network or CJARS VDE security mechanisms, or to perform network or keystroke monitoring.

    c. Disabling or removing security or protective software and other mechanisms and their associated logs from the CJARS VDE.

    d. Modification of the CJARS VDE, 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.

    e. Installation of software, changing configuration of the CJARS VDE, or connecting the CJARS VDE to an unauthorized computer.

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

g. Taking screenshots, pictures, transcribing, or otherwise duplicating images of the CJARS VDE or its interfaces. This includes data, whether original or derived, and the results of data analysis.

10. I acknowledge and consent to the following conditions when I access the CJARS VDE:

    a. The University of Michigan hosts the CJARS VDE and 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.

    b. The University of Michigan and/or CJARS may inspect, and if necessary remove, data stored on the CJARS VDE.

    c. Files created by the project team and stored in the project's workspace on the CJARS VDE are not private, are subject to routine monitoring and inspection, and may be disclosed to the sponsoring project, my employer, and any regulating bodies.

    d. The CJARS VDE includes security measures (e.g., authentication and access controls) to protect the sensitive data stored within--not for my personal benefit or privacy.

11. I will immediately report suspicious system activity or concerns to my CJARS VDE representative by emailing cjars-vde-users@umich.edu.

By signing this user agreement, I confirm that I have read and acknowledge the terms and conditions described above.

_____

RESEARCHER NAME TYPED OR PRINTED

_____

RESEARCHER SIGNATURE DATE