**Exhibit E: Data Management Plan**

The data management plan outlines how data will be used, stored, accessed, and protected. In addition, the plan contains how the output of the programmatic policy evaluation can be made accessible outside of the environment. The data management approach follows the five safes framework.

Safe projects. The design of the ADRF ensures that only approved projects which follow the relevant legal and ethical considerations are allowed (IRB if needed). **[AUXILIARY PARTY]** and class participants will get access to a contained safe workspace inside the ADRF. Access will only be granted to the data that class participants need for the program and is granted by  **[AUXILIARY PARTY]**. By policy, all class participants' access to projects is revoked upon completion of the project. Projects are then retained unless otherwise stated in this data sharing agreement.

Safe people. The best data protection is having responsible users. To achieve this the ADRF

promotes a culture of continuous and collaborative learning about how data can be accessed.

This learning starts with security trainings during onboarding, continuous refreshers, providing

interactive documentation and learning videos, to giving class participants access to collaborative spaces where they can help and learn from each other. Class participants will learn best practices and policies addressing safe data usage. For example, the security training informs them about confidentiality, personally identifiable information (PII), information security and regulations that mandate the protection of IT assets, personal responsibility and best practices to protect information systems from within their offices and when working remotely, and common threats to information and privacy and proper responses.

Safe data. Data will be de-identified as required by **[AUXILIARY PARTY]**: this means data sources do not contain any direct identifiers such as names, account numbers, or residential addresses. Direct identifiers will be hashed prior to being transmitted to the ADRF using the Hash-based Message Authentication Code (HMAC) algorithm. A random seed, known as a “salt” is used to create an encryption key that is then used to encrypt a “message”, which is then hashed using SHA256. The hashing is one way and cannot be ‘decrypted’ and allows for joins of hashed values in two different tables that used the same salt. This allows linkage across agency borders without compromising the privacy of the agencies’ clients.

Safe settings. The data will be hosted in the Administrative Data Research Facility (ADRF), a

secure computing environment in the cloud. The ADRF has achieved FedRAMP Moderate

certification, which is a government-wide program that provides a standardized approach to

security assessment, authorization, and continuous monitoring for cloud products and services.

ADRF is built on Amazon GovCloud, which is designed to host sensitive data and run regulated

workloads. GovCloud includes facilities for Virtual Private Cloud (VPC) in addition to the

benefits of scalable on-demand infrastructure. GovCloud also provides AWS Shield as an

always- on protection service that safeguards applications from Distributed Denial of Service

(DDoS) attacks. The ADRF is equipped with various tools and services for ongoing and

continuous security and infrastructure monitoring and administration. Key capabilities include

secure remote access, security scanning and vulnerability management, virus and malware

protection and application monitoring. ADRF also uses security APIs for encryption and identity

management. Overall ADRF adheres to all FedRAMP Moderate controls based on NIST

800–53 Revision 4 standards plus additional controls specific to cloud computing. A list of all technical security controls can be requested here: <https://marketplace.fedramp.gov/#/product/administrative-data-research-facility-adrf?sort=productName&productNameSearch=ADR>

Safe outputs. Work products to be exported from the project or user spaces must follow all relevant export policies from **[AUXILIARY PARTY]** in addition to the standard ADRF export process. ADRF operations will  follow its standard process for identifying export requests. The general flow of this process is:

(i) The participant creates a folder for a given export, then place files that need to be reviewed for export into that folder.

(ii) The participant submits the bundle of files in the folder for review

(iii) The participant iterates review and correction as needed until export is approved. Once export is approved, ADRF operations will:

a. record specific version of each file for export

b. package the files for export and

c. export out of the ADRF environment.

If  **[AUXILIARY PARTY]** has additional export process requirements, ADRF operations will work to incorporate these procedures and provide access to the appropriate agency personnel to oversee the export process.

Incidence response. The ADRF also has formal, documented incident response policies and

Procedures following the FedRAMP Continuous Monitoring Strategy. These policies and procedures mandate the process for ensuring security incidents, are properly identified, reported, and monitored for the system and its associated components. They address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policies are reviewed at least every three years and the procedures are reviewed at least annually; updates are made on an as needed basis.

Controlled workflows. All workflows that are directly associated with data are managed through the ADRF. This includes the ingestion of data, the actual data work, obtaining additional resources, documentation, knowledge exchange, export of output, provision of reports. The user interface is designed to promote collaboration, facilitate documentation, and provide information about data. This interactive design accelerates data-driven programmatic evaluation and policy around human beings and their interactions, for program management and policy development.

Data ingestion and curation. **[AUXILIARY PARTY]** can initiate a data transfer through the user interface and will then be guided through the ingestion process. All data files are encrypted for transmission to ADRF using a unique public-private key pair for each transfer. This public-private key pair used to encrypt these data are used for transfers associated for a given data provider, and will be deleted on completion of the transfer. This ensures that the data will be encrypted in motion up to the point of getting decrypted on the ADRF. Upon ingestion the data will be curated, metadata will be extracted and uploaded to the ADRF.

Data Retention and Removal. Data are retained only for as long as is necessary to accomplish the documented purpose for which the data were created or collected. Data are retained if the data usage agreement does not specifically preclude long-term archiving of the data. Data removal may take place as a result of the default retention period ending, a specific data agreement expiring, at the request of the Data Provider, or for other legal or regulatory compliance purposes. Data, regardless of the medium on which they are stored, will be destroyed, erased, or otherwise made unreadable prior to disposal. Restricted data are removed from all media using platform-appropriate utilities in order to ensure deletion from the system while also safeguarding from any attempt to reconstruct the data. Projects may contain subsets of datasets in the ADRF and are also subject to review and removal should access expire to a dataset used in a project. All user work on a project should take place in the project workspace and not in any given user’s home directory. Project removal will be conducted the same way that secure data are removed, using platform-appropriate utilities in order to ensure deletion from the system while also safeguarding from any attempt to reconstruct the data.

**FedRAMP Certification**

The ADRF FedRAMP Moderate level certification requires that all systems adhere to the regulations below and are regularly assessed by our third-party assessment organization. The controls defined in our System Security Plan are designed to safeguard the confidentiality, integrity and availability of data hosted on the platform.

**APPLICABLE LAWS AND REGULATIONS**

·         Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]

·         E-Authentication Guidance for Federal Agencies [OMB M-04-04]

·         Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]

·         Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]

·         Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMBM-01-05]

·         Homeland Security Presidential Directive-7,Critical Infrastructure Identification, Prioritization and Protection [HSPD-7]

·         Internal Control Systems [OMB Circular A-123]

·         Management of Federal Information Resources [OMB Circular A-130]

·         Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]

·         Privacy Act of 1974 as amended [5 USC 552a]

·         Protection of Sensitive Agency Information [OMB M-06-16]

·         Records Management by Federal Agencies [44 USC 31]

·         Responsibilities for the Maintenance of Records About Individuals by Federal Agencies

·         Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

**APPLICABLE STANDARDS AND GUIDANCE**

·         A NIST Definition of Cloud Computing [NIST SP 800-145]

·         Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]

·         Contingency Planning Guide for Federal Information Systems [NIST SP 800-34,Revision 1]

·         Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]

·         Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A, Revision 1]

·         Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18,Revision 1]

·         Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]

·         Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]

·         Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]

·         Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]

·         Managing Information Security Risk: Organization, Mission, and Information System View [NIST SP 800-39]

·         Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]

·         Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-2]

·         Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]

·         Guide for Conducting Risk Assessments [NIST SP 800-30, Revision 1]

·         Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]

·         Security Requirements for Cryptographic Modules [FIPS Publication 140-2]