Attachment B

Addendum Include within Technology Service Provider Agreements

Security of NeighborWorks America (NW) Data within Technology Service Provider Environment

1. "**Technology Service Provider"** agrees to implement data security measures that are consistent with industry best practices and standards so that it:
    a) Protects the privacy, confidentiality, integrity and availability of NW data;
    b) Protects against accidental, unauthorized, unauthenticated or unlawful access, copying, use, processing disclosure, alteration, transfer, loss or destruction of NW data;
    c) Complies with all applicable federal and state laws, rules, regulations, directives and decisions that are relevant to the handling, processing, and use of NW data in accordance with this Agreement.

2. **Risk Assessments.** "Technology Service Provider" shall perform comprehensive internal and external risk assessments (at least annually and/or after major changes) and provide results to NW.
    a) "Technology Service Provider" agrees to send completed ***Third Party – Information Gathering Questionnaire*** to NW for review prior to executing this agreement.
    b) "Technology Service Provider" agrees to provide NW with any information technology audit report as to provide an understanding of "Third Party" security controls and requirements in place currently. E.G. - System and Organization Controls (SOC) Type 2 Report
    c) Upon request by NW, "Technology Service Provider" agrees to provide NW with the results of their most recent vulnerability scans or penetration test conducted for review.
    d) Upon request by NW, "Technology Service Provider" agrees to allow NW or a mutually acceptable third party to conduct an information security control review as it pertains to the scope of service outlined within the agreement.

3. **Organizational Security Responsibility.** "Technology Service Provider" shall assign responsibility for information security management to a senior management officer or a designated data steward to maintain the security of NW data. "Technology Service Provider" will provide this point of contact information to NW. "Technology Service Provider" agrees to return NW data or provide NW with evidence of destruction of NW data upon end or termination of this agreement. This includes hard copy and all forms of electronic data including backups and archives. Upon request, "Technology Service Provider" will provide NW with their most current Privacy Policy.

4. **Third Party or Shared Hosting Service Provider.** If "Technology Service Provider" uses any third party or shared hosting service provider, the Technology Service Provider must require that the third party protects NW data to at least the same level as the service provider. NW requests to receive independent security assessment reports (e.g. – ISO 2700x Certification and Report,

SSAE 16 SOC Reports, Shared Assessment Program – Agreed Upon Procedures Review, PCI DSS Report on Compliance, or IT Audit – External) from those parties and\or hosting service providers. The third party must protect each entity's hosted environment and data. NW reserves the right to move NW data within its own data center at its discretion.

5. **Data Retention and eDiscovery**. Technology Service Provider s will provide means for NW to enforce its data retention policies on all data over which Technology Service Provider has custody or will enforce data retention policy on behalf of NW. This will require the Technology Service Provider to provide assurances that data including metadata and events when appropriate are retained for the duration of the retention period. It also requires the Technology Service Provider to provide assurances that all copies including backups and archives of expired data are thoroughly destroyed. NW program offices will coordinate with the Technology Service Provider to identify data which is in scope for retention and destruction. Technology Service Provider further agrees to comply with all reasonable eDiscovery requests.

6. **Classification of generated, collected and aggregated data.** When applicable, Technology Service Providers who generate, collect or aggregate data on behalf of NW shall coordinate with the program office to ensure that all new data or new data combinations which satisfy definition of Personally Identifiable Information (PII), as found in NeighborWorks America Award/Contract – Section H. Special Contract Requirements, are appropriately classified and protected. Generated data includes data which is produced by analysts or automatically by algorithms.

7. **Logging and event generation for applications.** Technology Service Provider and NW program office shall coordinate to identify security relevant data and activities in all applications. Technology Service Provider shall ensure that events are generated when sensitive data is accessed and security relevant activities take place. Technology Service Provider shall ensure that security events are logged, can be accessed by NW upon request, and that logs are retained as specified in Data Retention.

8. **Business Continuity (BCP) & Disaster Recovery (DRP) Planning.** In the event the Technology Service Provider ceases to provide the service, the Technology Service Provider shall provide sufficient advanced warning to facilitate the exportation of data and work product to NW. NW may require regular exportation or archiving of data and work product to satisfy NW's BCP / DRP plans.

9. **Security Incident / event notification.** Technology Service Provider shall notify NW of any security incident or event which has material effect on NW data within 72 hours of discovery. Technology Service Provider shall have in place a defined and practiced IR plan and procedures. NW reserves the right to prosecute culpable parties at its discretion when NW data is impacted. Technology Service Provider agrees to assist with all reasonable requests from NW, NW's incident response contractors or law enforcement in all necessary investigations.

10. **Jurisdiction of data storage.** Technology Service Provider shall ensure that all data stored and processed on behalf of NW is kept within the Jurisdiction of the United States of America. Data shall not be transmitted outside this jurisdiction at any time.

11. **Single Sign On (SSO) Capability.** Technology Service provider shall ensure that identity authentication and access to application can be through Single Sign-on integration using the current standards (e.g. - Security Assertion Markup Language: SAML)for exchanging authentication and access authorization identities between security domains . Technology service provider should have the ability to integrate Single Sign-On access through Windows Active Directory (AD) for NW employees and contractors.

Attachment B

Third Party Information Gathering Questionnaire
(to be completed by Third-Party Service Provider)

Company Information:

Question/Request	**Response**
Responder Name:	
Responder Job Title:	
Responder Contact Information:	
Date of Response:	
List the names and titles of any contributors that assisted in the formulation of the responses:	
What is the name of the parent or holding company?	
What is the company /business name?	
How long has the company been in business?	
Are there any material claims or judgements against the company?	
If Yes, please describe, including any impact it may have on the service being provided to NWA	
Which regulator supervises or examines the company (if any)?	

Does the company have an internal audit, risk management or compliance department with responsibility for identifying and tracking any outstanding internal, external or regulatory issues?	
What is the target date for the signed contract?	
What is the target program/service launch date?	
What type of data will be hosted or managed - Credit Card Number - CCN, Social Security Number - SSN , Personally Identifiable Information - PII?	
Is this a new service offering? If not how long has it been on the market?	

Question/Request	Response
Is this a shared service? (A shared service is provided on a multi-tenant vs. dedicated equipment)	
Shared:	
Dedicated:	
Other: Please explain	
Are any aspects of the service outsourced?	
If yes, describe what is outsourced, name of the contracted party, whether the outsourced service involves NWA information and the country of operation.	
Has the service been audited in the past year for any of the following:	
Privacy	
Information Security	
Disaster Recovery	
Operations	

Technology	
Other	
Does the company hire an external audit firm to provide produce a report on areas under review?	
If so, please explain what types of external audit has been conducted within the past year.	
Have any of the audits addressed above resulted in any significant exceptions or findings that have not been remediated ?	
If yes, please provide details:	
Provide an explanation of the NWA data and transaction that are part of your service?	
What is the production site physical address?	
What is the backup site physical address?	
Are there any additional location(s) where NWA data is stored?	
If so, provided locations (address, city , state, country).	
Please provide details in the following areas:	
Operation System (s)	
Question/Request	**Response**
Workstations # of devices	
Servers # of devices	
List of Applications in Scope	
Number of employees by function (e.g. development, systems operations, information security)	
Will there be CCN, SSN, PII data stored, processed or transmitted by the vendor or it's co-location center?	

Types of data that may be transmitted from the vendor to NWA and method:	
Types of data that may be transmitted from NWA to the vendor and method:	
Types of electronic connections between NWA and the vendor center:	
Types of electronic connections between NWA and the co-location center:	

Data and Access	**Response**
How data and metadata ingested from documents are classified (PII, financial, etc.)	
How data at rest and in transit is encrypted	
IAM: approach to role-based access controls	
Overview of data retention, backup, and recovery procedures	
Audit logging capabilities	
AI Model Security	**Response**
How data ingested will not be used outside of our workflow(s), including but not limited to, training other shared or public models	
Where our data and workflows will be stored in relation to another client's workspace	
Human validation requirements of model outputs	
How the results generated by the model are obtained, including specific sources.	

How the solution inherits and enforces existing SharePoint permissions and access controls across all integrated data sources	
AI Model Security	**Response**
Full disclosure of all third-party integrations	
API security: required OAuth 2.0 and SOC 2/ISO certifications, and other relevant certifications	