MEMORANDUM OF AGREEMENT
BETWEEN THE COUNTY OF ALBANY
AND THE CITY OF ALBANY

CONTRACT NO. 2292 OF 2024

PURSUANT TO RESOLUTION NO. 460 OF 2024

This Memorandum of Agreement is made by and between the County of Albany, a municipal corporation duly organized under the State of New York, acting by and through its County Executive, and having a principal place of business at 112 State Street, Albany, New York 12207 (hereinafter, the "County"), and the City of Albany, a municipal corporation duly organized under the laws of the State of New York, acting by and through its Mayor, and having a principal place of business at City Hall, 24 Eagle St, Albany, NY 12207 (hereinafter, the "City," and together with the County, may be referred to herein as the "[P]arties.").

WITNESSETH:

WHEREAS, it is a priority of the County to engage in cooperative efforts with other municipal entities in order to provide improved services to their residents; and

WHEREAS, the City is in need of a site location to use for data backup/recovery; and

WHEREAS, the County possesses data center space and fiber connectivity at 449 New Salem Road, Voorheesville, NY suitable to the City's needs; and

WHEREAS, the County has been providing the City with data center space and fiber connectivity for data backup/recovery since January 1, 2016 equivalent to that which will continue to be provided under this Memorandum of Agreement; and

WHEREAS, the City agrees to follow the policies and practices provided as an incorporated Addendum to this Memorandum of Agreement (together, the "Agreement"); and

WHEREAS, each governing body finds that the performance of this Agreement is in the best interests of all parties, that the undertaking will benefit the public, and that the division of costs fairly compensates the performing party for the services or functions under this Agreement; and

WHEREAS, the Albany County Legislature has authorized the Albany County Executive to enter into an Agreement with the City to provide the aforesaid services via Resolution No. 460 of 2024 (adopted 8/12/2024); and

NOW THEREFORE, in consideration of the mutual benefits conferred by this Memorandum of Agreement and Addendum, the parties hereby agree as follows:

SECTION I. SERVICES

1.1 The County shall provide data center space and fiber connectivity for the use as a data disaster recovery site to the City at 449 New Salem Road, Voorheesville, NY.

1.2 The County shall provide rack space, network connectivity and power in its specified Disaster Recovery Site.

1.3 The City shall provide its own equipment to include firewall protection, switch and data storage, as well as support and maintenance of the equipment at the aforementioned location, at no cost to the County. The County is not liable for any equipment or the maintenance and support for that equipment as provided by the City. The City is responsible for protecting and securing this equipment to include antimalware, security patches, and firmware updates within two (2) weeks of release.

1.4 The City shall be responsible for the cost of new hardware or services beyond what the County already has in place, including changing the infrastructure to accommodate the City and keep isolated from the County.

1.5 The City's physical access to the Albany County Disaster Recovery Site is limited to normal business hours. In an Emergency Disaster Recovery Situation, the County shall work with the City to provide physical access during non-business hours.

1.6 The City will follow and provide documentation of adherence to practices as required by the Addendum, Albany County Technology Procurement – City Administrative Terms & Conditions.

SECTION II. INDEMNIFICATION

The City shall defend, indemnify, and save harmless the County, its agents, representatives, and employees, from and against any and all claims, damages, losses, and expenses (including, but not limited to, reasonable attorney's fees) arising from the services rendered by the County in relation to this Agreement, provided, however, that the City shall not be obligated to indemnify the County for that portion of any claim, loss, or damage arising hereunder due to the negligent act or failure to act by the County.

SECTION III. EFFECTIVE DATE AND TERM

The services and terms outlined in this Agreement shall be retroactive to January 1, 2016 and continue until May 31, 2025 upon execution of this agreement.

SECTION IV. AMENDMENTS

This Agreement represents the entire agreement between the Parties and no amendments or additions thereto or modifications thereof have been agreed to or shall be binding hereafter, unless evidenced in writing by the Parties.

SECTION V. NOTICE

All notices to be given hereunder shall be given in writing and shall be delivered personally or by U.S. mail as follows:

If to the County of Albany:

Office of the County Executive
Albany County
112 State Street, Room
1200
Albany, NY 12207

If to the City of Albany, NY

Kathy M. Sheehan
Mayor
24 Eagle Street
Albany, New York 12207

SECTION VI. INSURANCE REQUIREMENTS

6.1 The City shall maintain insurance in an amount not less than the value of the equipment utilized in the completion of this Memorandum of Agreement.

6.2 The City shall also maintain insurance for Automobile, Bodily Injury, and Property damage for the equipment utilized in completing this Memorandum of

Agreement in an amount not less than ONE MILLION DOLLARS ($1,000,000.00) per occurrence subject to a THREE MILLION DOLLARS ($3,000,000.00) aggregate. The City will also maintain a minimum of ONE MILLION DOLLARS ($1,000,000) in Cyber Liability coverage.

6.3 Certificates of insurance shall be issued naming the County of Albany as certificate holder and primary/non-contributory additional insured as required by written contract.

6.4 The City shall provide Certificates of Insurance that fulfill the requirements of this Section before the services contemplated in this Memorandum of Agreement are commenced.

SECTION VII. ENTIRE AGREEMENT

This Memorandum of Agreement and incorporated Addendum represents the sole and entire agreement between the Parties and shall supersede any and all other agreements regarding the topic of this Agreement. The Parties acknowledge and agree that neither Party has made any representation with respect to the subject matter of this Agreement or any representations inducing the execution and delivery hereof except such representations as are specifically set forth herein and each of the Parties acknowledge that each has relied on its own judgment in entering into this Agreement. The Parties further acknowledge that any prior statements or representations made, if at all, are void and of no effect on this Agreement, and that neither Party has relied on such prior statements or representations in connection with this Agreement.

IN WITNESS WHEREOF, each of the Parties has duly signed this Memorandum of Agreement on the dates written below.

(REMAINDER OF PAGE INTENTIONALLY LEFT BLANK)

The County of Albany

By:______________________ 12/4/24

Date

Daniel P McCoy
County Executive
or
Michael P. McLaughlin
Deputy County Executive

The City of Albany

By:______________________ 11/13/24

Date

Kathy M. Sheehan
Mayor

NOTARY ACKNOWLEDGEMENT

STATE OF NEW YORK)
COUNTY OF ALBANY) ss.:
CITY OF ALBANY)

On this ______ day of ________________, 2024, before me personally came Daniel P. McCoy, to me known and known to me to be the Albany County Executive and the same person who executed the foregoing instrument; and they acknowledged that they executed the foregoing instrument on behalf of the County of Albany, New York as said Executive pursuant to the authority vested in them.

____
Notary Public, State of New York

NOTARY ACKNOWLEDGEMENT

STATE OF NEW YORK)
COUNTY OF ALBANY) ss.:
CITY OF ALBANY)

On this 4th day of December, 2024, before me personally came Michael P. McLaughlin, me known and known to me to be the Deputy County Executive and the same person who executed the foregoing instrument; and they acknowledged that they executed the foregoing instrument on behalf of the County of Albany, New York as said Executive pursuant to the authority vested in them.

EUGENIA K. CONDON
Notary Public, State of New York
Registration No 02CO4969817
Qualified in Albany County
Commission Expires July 23, 20[illegible]

____
Notary Public, State of New York

NOTARY ACKNOWLEDGEMENT

STATE OF NEW YORK)
COUNTY OF ALBANY) ss.:
CITY OF ALBANY)

On this 15th day of November, 2024, before me personally came Kathy Sheehan, to me known and known to me to be the Mayor of the City of Albany, New York, and the same person who executed the foregoing instrument; and she acknowledged that she executed the foregoing instrument on behalf of the City of Albany, New York, as said Mayor pursuant to the authority vested in her.

Shaniqua Jackson
Notary Public, State of New York
Reg. No. 01JA0017107
Qualified in Albany County
Commission Expires 11/29/2027

Shaniqua Jackson
____
Notary Public, State of New York

Addendum

Albany County Technology Procurement – City Administrative Terms & Conditions

1. Secure System Development Lifecycle and Specifications

Unless otherwise agreed to by the Authorized User (AU), "Albany County," in writing, the City's current version of the solution must function as specified in the associated Request for Proposal, Contract, or other agreement in an environment comprised solely of components including, but not limited to operating system and database platform versions which are in an active support phase (e.g., no requirement to run on End of Life software, such as Windows 7, etc.).

Unless otherwise agreed to by the Authorized User in writing, the City shall represent the below practices by providing the documentation of City's adherence to the below policies available in a public website or secure portal that shall be provided to Authorized Users upon request.

a) Secure System Development Lifecycle

i) Policies that govern software development practices commensurate with the risk of the intended use of each software component:

(1) Such policies shall define documented security roles for the software development team

(2) On no less than an annual basis, the City shall conduct a comprehensive review of software development policies and make changes where indicated to adequately address new or changed risk

ii) At least annually, the City shall provide training in secure software development practices to its developer workforce.

(1) Such training shall be focused on the technologies in use within the software development environment

(2) Such training shall include a review of the City's chosen secure coding framework (see "Vulnerability Management" section) and related policies, procedures and standards

(3) Such training shall include a review of the security-related roles and responsibilities conferred on development personnel by organizational policy

iii) The City shall, to the extent legally permissible, conduct criminal background checks, credit checks and reference checks for all personnel engaged in the software development process, and establish a set of criteria for when management must be engaged regarding the results of such checks.

iv) The City shall deliver remote and /or on premises support only with approval of AU and with the option for AU to supervise / observe the support activity

v) At no time during remote and /or on premises support, or any other time, shall City transfer AU's data from AU's on premise installation to a remote location without the express written permission of the AU

vi) The City shall 1) utilize uniquely assigned credentials for each of its workforce members to be used in supporting the AU's solution and 2) revoke those credentials within 24 hours of the departure of a City's workforce member who had knowledge of credentials used to support the AU's solution or notify the AU within 24 hours if the credentials used exist on an AU on-premise system. Credential management must be in accordance with NIST 800-63-3, Digital Identity, or its successor.

vii) Upon request and with reasonable notice, the City shall provide the AU with a list of its workforce members with knowledge of credentials used to access the AU's solution.

b) Vulnerability Management

i) The City shall make commercially reasonable efforts to ensure that components including but not limited to third party libraries, components and APIs are maintained at their most recent, stable version within the released application made available to the AU.

ii) The City shall follow a secure coding framework appropriate to the nature of its software components. For example, web application development teams may follow the Open Web Application Security Project's Secure Coding Practices

iii) The City shall document and execute a remediation plan for any vulnerability identified through dynamic or static analysis, vulnerability scans or penetration tests, where the vulnerability has a CVSS severity of 7.0 or higher

iv) The City shall establish processes for monitoring and acting upon vulnerability notices published regarding components of the software development environment as well as components used in the solution provided to the AU

v) The City shall maintain publicly available mechanisms for receiving reports of vulnerabilities identified by its customers, security researchers and similar entities.

c) Application Lifecycle Management

i) The City shall ensure that any open source licenses which apply to components used in the solution confer no obligations upon the AU, or that in the event of such obligation, the AU is aware of and agrees to same.

ii) All applications released by City to the AU shall be signed by a publicly trusted code signing certificate so that the AU may verify the authenticity and integrity of the release. This code signing certificate shall be rotated on at least an annual basis.

iii) The City shall ensure that all implementation services and / or guides comprehensively address security hardening for the solution. Such hardening shall include, but not be limited to, the disabling of unnecessary features based on the Scope of Work and the implementation of a "least privilege" access model for all users and service accounts.

iv) The City shall implement processes to ensure that all changes to the solution:

(1) Are made at the direction of its product managers or equivalent role

(2) Are documented in a work management / issue tracking application

(3) Maintain evidence of security checks and approvals

(4) Include documented functional requirements and non-functional security requirements

(5) Include a plan for notifying customers, including the AU, of any substantive changes upon release

v) The City shall provide ample notice, and in no case less than six months, should the solution version used by the AU reach End of Life, such that it will no longer receive security updates to address vulnerabilities.

d) Specifications

During the term of the Contract, the Authorized User may request Product specifications for particular items that have been included by the City on its approved price list for the Contract. These specifications will be provided by the City at no cost.

2. Instruction Manuals and Associated Documentation

Product shall be furnished, at no extra charge, with one complete set of standard operator instruction manuals and Documentation (hard copy, CD/DVD, or web link) as would normally accompany such Product. City shall also ensure that the part numbers and net prices associated with the documentation are available to the Authorized User and included on its approved price list for this Contract should an Authorized User need to purchase additional sets of technical manuals. Where Documentation is provided in electronic format, an Authorized User shall be entitled to make copies to the extent necessary to fully enjoy the rights granted under this Contract provided that the Authorized User reproduces the copyright notice and any other legend of ownership on any copies made.

3. Security

a) Security Incidents

The Authorized User and the City must, in writing, determine a Security Incident notification policy prior to the finalization of the Authorized User Agreement. If no such agreement is in place, then the default agreement shall be notification of all Security Incidents that may have a direct impact on the AU by phone immediately upon detection to the Authorized User representative.

All AU notifications will be followed with a notification to the Albany County Chief Information Officer.

If requested in the Authorized User agreement and agreed to by the City, a written preliminary incident analysis report must be provided to AU within 72 hours of discovery.

City representative must be available by phone and email for discussions with the Albany County Chief Information Officer and AU representative throughout incident response activity and must provide status updates at mutually agreed upon cadences. A written final incident analysis report, including a detailed technical section including root cause of incident, timeline, scope, impact and corrective actions taken must be delivered to AU at the conclusion of incident response.

b) Data Breach – Required City Actions

Unless otherwise provided by law, in the event of a Data Breach, the City shall:

i) notify the Albany County Chief Information Officer, the Albany County Cyber Incident Response Team, and any potentially affected Authorized User's representative, by telephone as soon as possible from the time the City confirms Data Breach. An Authorized User may specify a maximum notification time in their RFQ or RFP;
ii) consult with and receive authorization from the Authorized User as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required, either by statute or by the Authorized User;
iii) coordinate all communication regarding the Data Breach with the Albany County Chief Information Officer and Authorized User (including possible communications with third parties);
iv) cooperate with the Authorized User, Albany County Chief Information Officer, Albany County Division of Information Services and any City working on behalf of the Authorized User or Albany County in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and
v) promptly take commercially reasonable steps to mitigate the effects and minimize any damage resulting from the Security Event. City shall provide Written notice to the Authorized User as to all such corrective actions taken by the City to remedy the Data Breach. Unless otherwise agreed to in the Authorized User Agreement, if City is unable to complete the corrective action within the required timeframe, the Authorized User may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the Authorized User, or until the Authorized User has completed a new procurement for a replacement service system; (ii) and the City will be responsible for the reasonable cost of these services during this period.

Nothing herein shall in any way (a) impair the authority of the Office of the Attorney General or other investigative or law enforcement entity to bring an action against City to enforce the provisions of the New York State Information Security Breach

Notification Act (ISBNA) or (b) limit City's liability for any violations of the ISBNA or any other applicable statutes, rules or regulations.

c) Location of Data; CONUS or OCONUS

i) The RFQ or RFP must specify if the AU will allow Data to be located outside of the Continental United States (OCONUS).

ii) Unless otherwise authorized in the RFQ and agreed to in the Authorized User Agreement, when the City is responsible for managing the Data, the City shall meet the following requirements:

a. All Data shall remain in the Continental United States (CONUS).

b. Any Data stored, or acted upon, shall be solely located in Data Centers within CONUS.

c. Any services which directly or indirectly access Data shall be performed only from locations within CONUS.

d. All Data in transit shall remain in CONUS and shall be encrypted in accordance with generally accepted standards.

e. All helpdesk, online and support services which may access Data shall be performed only from locations within CONUS.

f. No Follow the Sun support shall be allowed to access Data directly or indirectly from locations outside CONUS.

iii) Unless otherwise authorized in the RFQ or RFP and agreed to in the Authorized User Agreement, when the Authorized User is responsible for managing the Data, the City shall provide the Authorized User with the capability and the means or tools to meet the following requirements:

a. All Data shall remain in the Continental United States (CONUS).

b. Any Data stored, or acted upon, shall be solely located in Data Centers within CONUS.

c. Any services which directly or indirectly access Data shall be performed only from locations within CONUS.

d. All Data in transit shall remain in CONUS and shall be encrypted in accordance with generally accepted standards.

e. All helpdesk, online and support services which may access Data shall be performed only from locations within CONUS.

f. No Follow the Sun support shall be allowed to access Data directly or indirectly from locations outside CONUS.

iv) Unless otherwise authorized in the RFQ or RFP and agreed to in the Authorized User Agreement, City may not store, act upon, or access Data outside of the Continental United States (OCONUS) and may not perform support services that may access Data from OCONUS.

Authorized Users must receive prior written approval from the Albany County Chief Information Officer, before authorizing Data to be stored, acted upon, or accessed OCONUS, and before authorizing support services to be performed from OCONUS.

v) Notwithstanding the foregoing, all services must be performed within CONUS and may not be authorized to be performed from OCONUS.

d) Security Reports

City must log in accordance with NIST 800-92, or its successor. Upon request, the City must provide the Authorized User with security logs and reports (such as SOC2 Type 2, CAIQ, and ISO27001) to allow the Authorized User to make an informed decision about the City's security controls and their effectiveness.

City shall cooperate with all reasonable Authorized User requests for a written description of City's physical/virtual security and/or internal control processes. The Authorized User shall have the right to reject any City's RFQ or RFP response or terminate an Authorized User Agreement when such a request has been denied.

e) Support Services

All helpdesk, online, and support services which access any Data must be performed from within CONUS, unless expressly authorized by the Authorized User in writing. Unless such authorization is granted, at no time will any Follow the Sun support be allowed to access Data directly, or indirectly, from outside CONUS. If an Authorized User agrees to OCONUS services that access Data, then the Authorized User must be provided any information requested such as security reports (e.g. SOC2 Type 2, CAIQ and ISO27001) to allow the Authorized User to make an informed decision about the security of the Data in that location.

f) Infrastructure Support Services

Infrastructure support services that do not directly or indirectly access Data may be provided in a Follow the Sun format, if expressly outlined within the Authorized User Agreement.

g) Requests for Data By Third Parties

Unless prohibited by law, City shall notify the Authorized User in writing within 24 hours of any request for Data (including requestor, nature of Data requested and timeframe of response) by a person or entity other than the Authorized User, and the City shall secure Written acknowledgement of such notification from the Authorized User before responding to the request for Data.

Unless compelled by law, the City shall not release Data without the Authorized User's prior written approval.

h) Security Policies

City must maintain records documenting adherence to the following security policies and must provide such records to an Authorized User, or to the Albany County Chief Information Officer or Division of Information Services, upon request, through a public website or secure portal.

Policies that govern software development practices commensurate with the risk of the intended use of each software application

- Such policies shall define documented security roles for the software development team
- On no less than an annual basis, the City shall conduct a comprehensive review of software development policies and make changes where indicated to adequately address new or changed risk

The City shall deliver remote and /or on premises support only with approval of AU and with the option for AU to supervise / observe the support activity

At no time during remote and /or on premises support, or any other time, shall City transfer AU's data from AU's on premise installation of the software application to a remote location without the express written permission of the AU

The City shall 1) utilize uniquely assigned credentials for each of its workforce members to be used in supporting the AU's software application or 2) notify the AU within 24 hours of the departure of a City's workforce member who had knowledge of credentials used to support the AU's software application.

Upon request and with reasonable notice, the City shall provide the AU with a list of its workforce members with knowledge of credentials used to access the AU's software application

The City shall make commercially reasonable efforts to ensure that components including but not limited to third party libraries, components and APIs are maintained at their most recent, stable version within the released application made available to the AU.

The City shall follow a secure coding framework appropriate to the nature of its software application. For example, web application development teams may follow the Open Web Application Security Project's Secure Coding Practices

The City shall document and execute a remediation plan for any vulnerability identified through dynamic or static analysis, vulnerability scans or penetration tests, where the vulnerability has a CVSS severity of 4.0 or higher

The City shall establish processes for monitoring and acting upon vulnerability notices published regarding components of the software development environment as well as components used in the software application provided to the AU

The City shall maintain publicly available mechanisms for receiving reports of vulnerabilities identified by its customers, security researchers and similar entities.

The City shall ensure that any open source licenses which apply to components used in the software application confer no obligations upon the AU, or that in the event of such obligation, the AU is aware of and agrees to same.

All applications released by City to the AU shall be signed by a publicly trusted code signing certificate so that the AU may verify the authenticity and integrity of the release. This code signing certificate shall be rotated on at least an annual basis.

The City shall ensure that all implementation guides and training comprehensively address security hardening for the application. Such hardening shall include, but not be limited to, the disabling of unnecessary features based on the Scope of Work and the implementation of a "least privilege" access model for all users and service accounts.

The City shall implement processes to ensure that all changes to the software application:

- Are made at the direction of its product managers or equivalent role
- Are documented in a work management / issue tracking application
- Maintain evidence of security checks and approvals
- Include documented functional requirements and non-functional security requirements
- Include a plan for notifying customers, including the AU, of any substantive changes upon release

In no case shall the City knowingly release to the AU an application which contains a vulnerability with a CVSS severity of 7.0 or higher, without the direct written permission of the AU.

i) Secure Data Disposal

After 60 calendar days from expiration or termination of an Authorized User Agreement, or at a time mutually agreed upon by the Authorized User and the City, the City shall destroy Data in all of its forms, including all back-ups. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) 800-88, or its successor, as designated by the Authorized User, as applicable. If requested by the Authorized User, certificates of destruction, in a form acceptable to the Authorized User, shall be provided by the City to the Authorized User.

j) Authentication Tokens

If included in an RFQ or RFP, the Authorized User Agreement may require authentication tokens for all systems in accordance with NIST 800-63B Authentication and Lifecycle Management, or its successor.