CITY OF FAIRFIELD
TECHNOLOGY SOFTWARE-AS-A-SERVICE (SaaS) AGREEMENT FOR NEOGOV SUITE of PRODUCTS WITH GOVERNMENTJOBS.COM, INC.

This AGREEMENT is made at Fairfield, California, as of ________, 2024 (the "Effective Date"), by and between the City of Fairfield, a municipal corporation (the "City") and GovernmentJobs.com, INC. ("Service Provider"), who agree as follows:

1) SERVICES. Subject to the terms and conditions set forth in this Agreement, Service Provider shall provide to the City the services ("Services") described in Exhibit "A" (the "Scope of Services"), which consists of the following: (a) Exhibit A-1 – Statement of Work (b) Exhibit A-2 – NeoGov Order Form. Service Provider shall provide Services at the time, place, and in the manner specified in Exhibit "A."

2) PAYMENT. City shall pay Service Provider for the Services rendered pursuant to this Agreement at the times and in the manner set forth in Exhibit "B." The payments specified in Exhibit "B" shall be the only payments to be made to Service Provider for Services rendered pursuant to this Agreement. Service Provider shall submit all billings for said Services to the City in the manner specified in Exhibit "B."

3) FACILITIES AND EQUIPMENT. Service Provider shall, at its sole cost and expense, furnish all facilities and equipment which may be required for furnishing Services pursuant to this Agreement.

4) COMPLETE AGREEMENT. The provisions set forth in Exhibits "A," "B," "C," "D," and "E" are part of this Agreement. In the event of any inconsistency between the general provisions of Exhibit "C" and any other terms or conditions of this Agreement, the provisions set forth in Exhibit "C" shall control. All provisions in this Agreement control over any provision in Exhibit "A." In the event of a disagreement among the documents comprising Exhibit "A," Exhibit A-1 controls over Exhibit A-2.

5) INSURANCE REQUIREMENTS. The insurance requirements set forth in Exhibit "D" are part of this Agreement. Notwithstanding any other provision to the contrary, in the event of any inconsistency between any other terms or conditions of this Agreement, the requirements set forth in Exhibit "D" shall control.

6) BUSINESS LICENSE. The Service Provider shall obtain and keep current a business license for work within the City of Fairfield pursuant to Chapter 10B of the Fairfield City Code, with respect to the gross receipts received pursuant to this Agreement. No payments shall be made to any Service Provider until such business license has been obtained, and all fees paid therefore, by the Service Provider. Business license applications and information may be obtained from the Community Development Department, Fairfield City Hall, 1000 Webster Street, Fairfield, CA 94533-4883, (707-428-7509) and online at www.fairfield.ca.gov/biz.

7) EXHIBITS. All exhibits referred to herein are attached hereto and are by this reference incorporated herein.

8) TERM. This Agreement shall be effective upon the Effective Date and shall remain in effect for a period of three (3) years following the Effective Date (the "Initial Term"). Following the Initial Term, this Agreement shall automatically renew for additional one (1) year terms, unless terminated pursuant to this Agreement or the City Manager, or his/her designee, provides Service Provider written notice of the City's intent to not renew the Agreement.

9) Where applicable, vehicles with a gross vehicle weight rating ("GVWR") greater than 8,500 lbs. and light-duty package delivery vehicles operated in California may be subject to the California Air Resources Board Advanced Clean Fleets regulations. Such vehicles may therefore be subject to requirements to reduce emissions of air pollutants. For more information, please visit the CARB Advanced Clean Fleets webpage at https://ww2.arb.ca.gov/our- work/programs/advanced-clean-fleets.

EXECUTED as of the day first above-stated.

City of Fairfield, a municipal corporation

By:________________________________
(signature)

Printed: ______________________________

Service Provider

DocuSigned by:

By:________________________________
C48A2B32DE9F457...
(signature)

NEOGOV LEGAL
RM
2:57 pm, Sep 11 2024

Printed: Alex Chun

EXHIBIT “A”

SCOPE OF SERVICES

Services are described more particularly in the following exhibits, which comprise this Exhibit A:

Exhibit A-1 – Statement of Work
Exhibit A-2 – NeoGov Order Form

Exhibit "A-1"

Statement of Work

1.0 DEFINITIONS: In this Agreement, the following terms have the following meanings, and all other capitalized terms have the meaning given to them elsewhere in this Agreement:

1.01 **"Authorized Persons"** as used in this document means the Service Provider's employees, contractors, subcontractors or other agents who need to access the Public Jurisdiction's personal data to enable the Service Provider to perform the Services required.

1.02 **"Data Breach"** as used in this document means the unauthorized access by non-authorized person/s that result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

1.03 **"Follow-the-sun"** is a workflow model in which work is passed on to the offices located in different time zones. In this way work is done round-the-clock thereby reducing the support duration and increasing the responsiveness.

1.04 **"Non-Public Data"** means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

1.05 **"Personal Data**" means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g. Social Security, driver's license, passport); financial account information, including account number, creditor debit card numbers; or protected health information (PHI) relating to a person.

1.06 "**Personally Identifiable Information**" **(PII)** PII refers to a combination of data elements (e.g. Social Security number, driver's license or other government-issued identification number, passport number, financial account number, or credit or debit card number in combination with security codes) that, when linked to the individual's first name or first initial and their last name, and not encrypted or otherwise could lead to the loss, theft or unauthorized use of the individual's personal information.

1.07 "**Platform Data"** shall mean any anonymized data reflecting the access to or use of the Services by or on behalf of the Public Jurisdiction or any user, including statistical or other analysis and performance information related to the provision and operation of the Services including any end user visit, session, impression, clickthrough or click stream data, as well as log, device, transaction data, or other analysis, information, or data based on or derived from any of the foregoing.

1.08 “**Public Jurisdiction**” means the City of Fairfield.

1.09 “**Public Jurisdiction Data**” as used in this document means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction’s hardware; the Service Provider’s hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the Service Provider.

1.10 “**Public Jurisdiction Identified Contact**” means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

1.10 **“Security Incident”** means the potentially unauthorized access by non-authorized persons to personal data or non-public data that could reasonably result in the use, disclosure or theft of a public jurisdiction’s unencrypted personal data or non-public data within the possession or control of a Service Provider. A security incident may or may not turn into a data breach.

1.11 “**Service Level Agreement**” **(SLA)** means a written agreement between both the public jurisdiction and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises (i.e., metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed and (6) any remedies for performance failures.

1.12 “**Service Provider**” means the contractor and its employees, subcontractors, agents and affiliates who are providing the Services agreed to under the contract.

1.13 **“Software-as-a-Service” (SaaS)** means the capability provided to the consumer to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

1.14 **“Statement of Work”** is a written statement in a solicitation document or contract that describes the public jurisdiction’s service needs and expectations.

2.0 DESCRIPTION OF SERVICES

2.1 Scope of Services

The Scope of Services to be performed by Service Provider under this Agreement is as described in this Statement of Work in Exhibit A of this Agreement.

2.2 Data Ownership

The public jurisdiction will own all right, title and interest in its data that is related to the Services provided by this contract. Service Provider shall not access public jurisdiction user accounts or public jurisdiction data, except
(1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

2.3 Data Protection

Protection of personal privacy and data shall be an integral part of the business activities of the Service Provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a. The Service Provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Service Provider applies to its own personal data and non-public data of similar kind.

b. All data obtained by the Service Provider in the performance of this contract shall become and remain the property of the public jurisdiction.

c. All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Service Provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the SLA, or otherwise made a part of this contract.

d. Unless otherwise stipulated, the Service Provider shall encrypt all non-public data at rest and in transit. The public jurisdiction shall identify data it deems as non-public data to the Service Provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.

e. At no time shall any data or processes – that either belong to or are intended for the use of a public jurisdiction or its offers, agents or employees – be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the public jurisdiction.

f. The Service Provider shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

g. The Service Provider shall exclusively own all right, title and interest in and to all Platform Data. City acknowledges Service Provider may compile Platform Data based on Public Jurisdiction Data input into the Services. City agrees that Service Provider may use Platform Data to the extent and in the manner permitted under applicable law. Such anonymized data identifies neither the public jurisdiction nor its users, nor can Public Jurisdiction or any of its users be derived from such data.

2.4 Data Location

The Service Provider shall provide its Services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The Service Provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Service Provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The Service Provider may provide technical user support on a 24/7 basis using a “Follow the Sun” model, unless otherwise prohibited in this contract.

2.5 Security Incident

Service Provider shall inform the public jurisdiction of any security incident or data breach.

a. Incident Response: The Service Provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of Service Provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. Security Incident Reporting Requirements: The Service Provider shall report a security incident to the appropriate public jurisdiction identified contact immediately as defined in the SLA.

c. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the Service Provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 72 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

2.6 Breach Responsibilities

This section only applies when a data breach occurs with respect to Personal Data within the possession or control of the Service Provider.

a. The Service Provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Service Provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 72 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a data breach. The Service Provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of the Service Provider's breach of its contract obligation to encrypt Personal Data or otherwise prevent its release, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonable determined by Service Provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

2.7 Notification of Legal Requests

The Service Provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The Service Provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

2.8 Termination and Suspension of Service

a. Public Jurisdiction may export or delete Public Jurisdiction Data from the Services at any time during a subscription term, using the existing features and functionality of the Services. Public Jurisdiction is solely responsible for its data retention obligations with respect to Public Jurisdiction Data. If and to the extent Public Jurisdiction cannot export or delete Public Jurisdiction Data stored on Service Provider’s systems using the then existing features and functionality of the Services, Service Provider will, upon Public Jurisdiction's written request, make the Public Jurisdiction Data available for export by Public Jurisdiction or destroy the Public Jurisdiction Data. If Public Jurisdiction requires the Public Jurisdiction Data to be exported in a different format than provided by Service Provider, such additional services will be subject to a separate agreement on a time and materials basis. Except as otherwise required by applicable law, Service Provider will have no obligation to maintain or provide any Public Jurisdiction Data more than ninety (90) days after the expiration or termination of this Agreement. Public Jurisdiction acknowledges that it is solely responsible for determining any retention requirements with respect to the Public Jurisdiction Data as required by applicable law and Service Provider disclaims all liability in connection with such determination. In addition, to the extent Public Jurisdiction requests that Service Provider retain Public Jurisdiction Data beyond the expiration of the retention period required by applicable law, rule or regulation, Service Provider disclaims all liability in connection with retaining such Public Jurisdiction Data including but not limited to any claims related to loss or destruction of such Public Jurisdiction Data. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the Services, unless a unique data retrieval arrangement has been established as part of the SLA.

b. The Service Provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

2.9 Background Checks

The Service Provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the public jurisdiction’s information among the Service Provider’s employees and agents.

2.10 Access to Security Logs and Reports

The Service Provider shall provide reports to the public jurisdiction in a format as specified in the SLA agreed to by both the Service Provider and the public jurisdiction. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this contract.

2.11 Contract Audit

The Service Provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense. Such audits shall occur no more than once in any 12-month period, and in a manner that does not unreasonably interfere with Service Provider's business operations. The public jurisdiction shall not conduct an audit on the physical premises or on servers where no personal or confidential information belonging to Public Jurisdiction is stored.

2.12 Data Center Audit

The Service Provider shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The Service Provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

2.13 Change Control and Advance Notice

The Service Provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

2.14 Security

The Service Provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the Service Provider. For example: virus checking and port sniffing — the public jurisdiction and the Service Provider shall understand each other's roles and responsibilities.

2.15 Non-disclosure and Separation of Duties

The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

2.16 Import and Export of Data

The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Service Provider. This includes the ability for the public jurisdiction to import or export data to/from other Service Providers.

2.17 Responsibilities and Uptime Guarantee

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the Services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Service Provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime),and provide service to customers as defined in the SLA.

2.18 Subcontractor Disclosure

The Service Provider shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, and who shall be involved in any application development and/or operations.

2.19 Right to Remove Individuals

The public jurisdiction shall have the right at any time to require that the Service Provider remove from interaction with public jurisdiction any Service Provider representative who the public jurisdiction believes is detrimental to its working relationship with the Service Provider. The public jurisdiction shall provide the Service Provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the Service Provider shall immediately remove such individual. The Service Provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

2.20 Business Continuity and Disaster Recovery

The Service Provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of 24 hours is met.

2.21 Compliance with Accessibility Standards

The Service Provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

2.22 Web Services

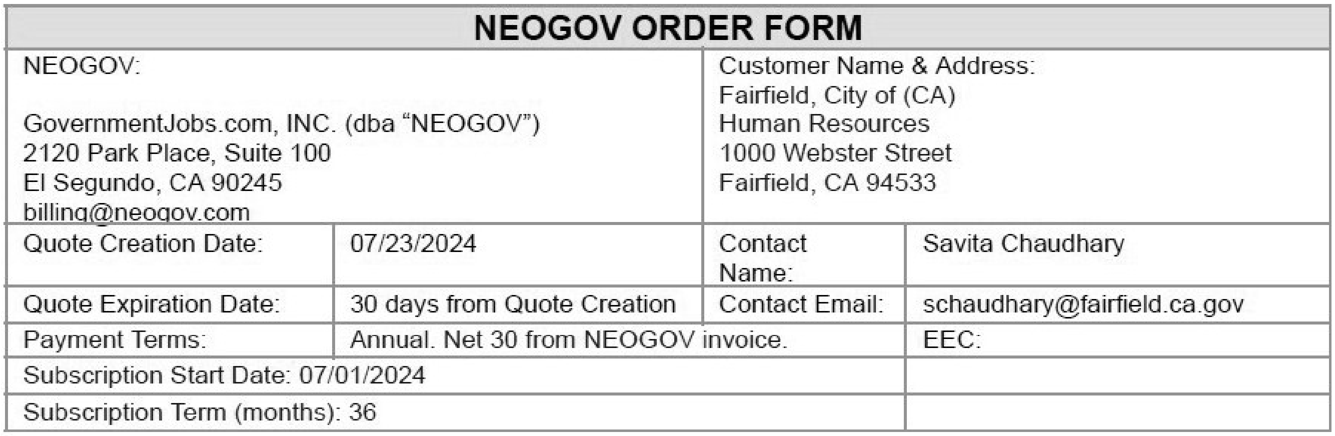
The Service Provider shall use Web services exclusively to interface with the public jurisdiction's data in near real time when possible.

2.23 Encryption of Data at Rest

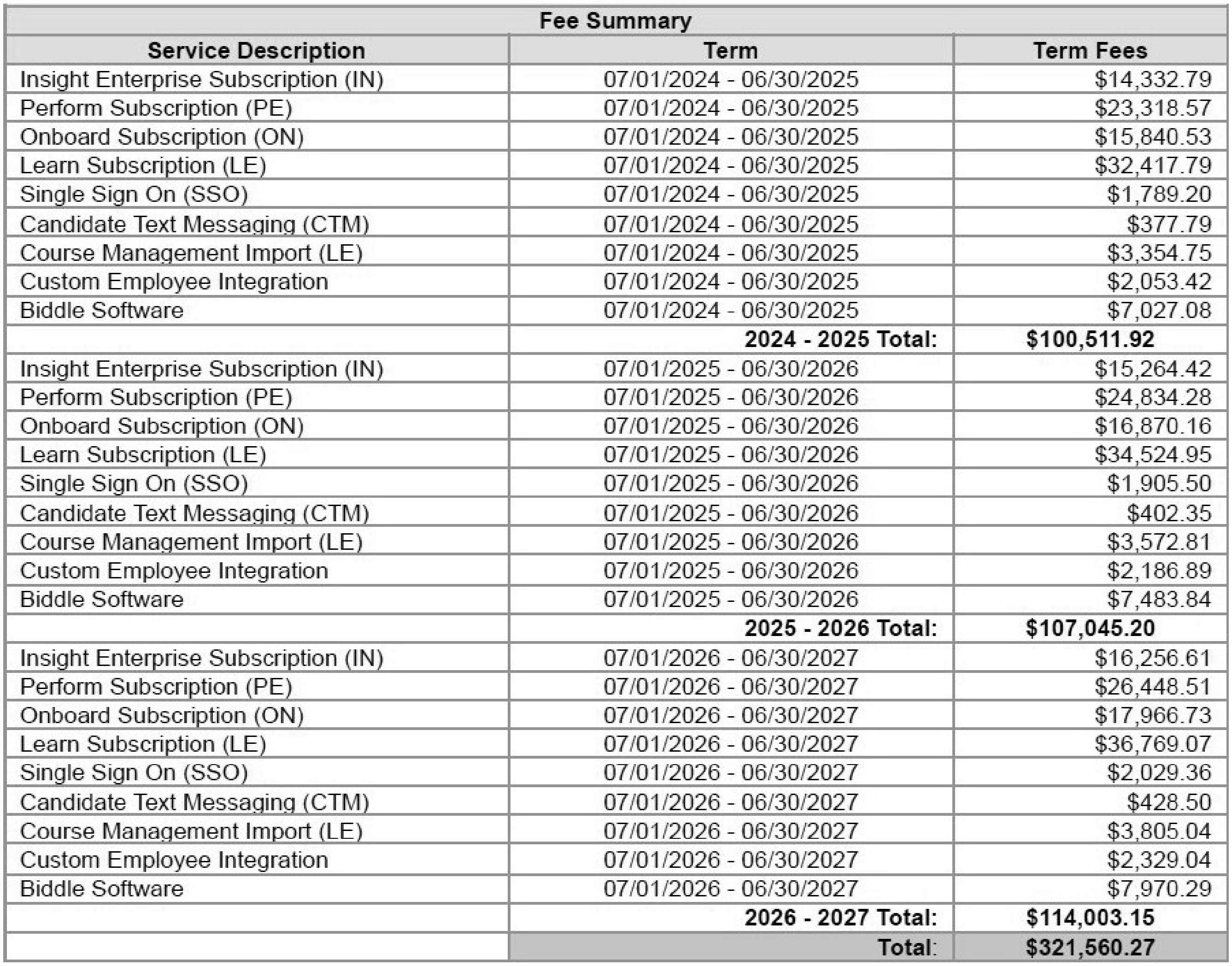
The Service Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data, unless the public jurisdiction approves the storage of personal data on a Service Provider portable device in order to accomplish work as defined in the statement of work.

Exhibit “A-2”

NeoGov Order Form



NEOGOV ORDER FORM			
NEOGOV: GovernmentJobs.com, INC. (dba “NEOGOV”) 2120 Park Place, Suite 100 El Segundo, CA 90245 billing@neogov.com		Customer Name & Address: Fairfield, City of (CA) Human Resources 1000 Webster Street Fairfield, CA 94533	
Quote Creation Date:	07/23/2024	Contact Name:	Savita Chaudhary
Quote Expiration Date:	30 days from Quote Creation	Contact Email:	schaudhary@fairfield.ca.gov
Payment Terms:	Annual. Net 30 from NEOGOV invoice.		EEC:
Subscription Start Date: 07/01/2024			
Subscription Term (months): 36			



Fee Summary		
Service Description	**Term**	**Term Fees**
Insight Enterprise Subscription (IN)	07/01/2024 - 06/30/2025	$14,332.79
Perform Subscription (PE)	07/01/2024 - 06/30/2025	$23,318.57
Onboard Subscription (ON)	07/01/2024 - 06/30/2025	$15,840.53
Learn Subscription (LE)	07/01/2024 - 06/30/2025	$32,417.79
Single Sign On (SSO)	07/01/2024 - 06/30/2025	$1,789.20
Candidate Text Messaging (CTM)	07/01/2024 - 06/30/2025	$377.79
Course Management Import (LE)	07/01/2024 - 06/30/2025	$3,354.75
Custom Employee Integration	07/01/2024 - 06/30/2025	$2,053.42
Biddle Software	07/01/2024 - 06/30/2025	$7,027.08
	2024 - 2025 Total:	**$100,511.92**
Insight Enterprise Subscription (IN)	07/01/2025 - 06/30/2026	$15,264.42
Perform Subscription (PE)	07/01/2025 - 06/30/2026	$24,834.28
Onboard Subscription (ON)	07/01/2025 - 06/30/2026	$16,870.16
Learn Subscription (LE)	07/01/2025 - 06/30/2026	$34,524.95
Single Sign On (SSO)	07/01/2025 - 06/30/2026	$1,905.50
Candidate Text Messaging (CTM)	07/01/2025 - 06/30/2026	$402.35
Course Management Import (LE)	07/01/2025 - 06/30/2026	$3,572.81
Custom Employee Integration	07/01/2025 - 06/30/2026	$2,186.89
Biddle Software	07/01/2025 - 06/30/2026	$7,483.84
	2025 - 2026 Total:	**$107,045.20**
Insight Enterprise Subscription (IN)	07/01/2026 - 06/30/2027	$16,256.61
Perform Subscription (PE)	07/01/2026 - 06/30/2027	$26,448.51
Onboard Subscription (ON)	07/01/2026 - 06/30/2027	$17,966.73
Learn Subscription (LE)	07/01/2026 - 06/30/2027	$36,769.07
Single Sign On (SSO)	07/01/2026 - 06/30/2027	$2,029.36
Candidate Text Messaging (CTM)	07/01/2026 - 06/30/2027	$428.50
Course Management Import (LE)	07/01/2026 - 06/30/2027	$3,805.04
Custom Employee Integration	07/01/2026 - 06/30/2027	$2,329.04
Biddle Software	07/01/2026 - 06/30/2027	$7,970.29
	2026 - 2027 Total:	**$114,003.15**
	Total:	**$321,560.27**

EXHIBIT "B"

PAYMENT

1. The price for Services rendered by Service Provider of the following:

a. Insight Enterprise Subscription
b. Perform Subscription
c. Onboard Subscription
d. Learn Subscription
e. Single Sign On (SSO)
f. Candidate Text Messaging
g. Course Management Import
h. Custom Employee Integration
i. Biddle Software

shall be the following for the 3-year period:

Year 1 – July 1, 2024 to June 30, 2025	$100,511.92
Year 2 – July 1, 2025 to June 30, 2026	$107,045.20
Year 3 – July 1, 2026 to June 30, 2027	$114,003.15
Total	**$321,560.327**

2. City shall pay Service Provider within 30 days after receipt of Service Provider's invoice.

3. The obligation to pay for Services commences on the Effective Date.

4. NON-REIMBURSABLE EXPENSES

Service Provider shall be responsible for all costs and expenses incurred by Service Provider, personnel of Service Provider and subcontractors of Service Provider, in connection with this Agreement, including, without limitation, payment of salaries, fringe benefit contributions, payroll taxes, withholding taxes, and other taxes or levies, office overhead expenses, travel expenses, telephone and other telecommunication expenses, and document reproduction expenses.

EXHIBIT "C"

GENERAL PROVISIONS

1) INDEPENDENT SERVICE PROVIDER. At all times during the term of this Agreement, Service Provider shall be an independent contractor and shall not be an employee of City. City shall have the right to control Service Provider only insofar as the results of Service Provider's Services rendered pursuant to this Agreement; however, City shall not have the right to control the means by which Service Provider accomplishes Services rendered pursuant to this Agreement.

2) LICENSES; PERMITS; ETC. Service Provider represents and warrants to City that Service Provider has all licenses, permits, qualifications, and approvals of whatsoever nature which are legally required for Service Provider to practice Service Provider's profession. Service Provider represents and warrants to City that Service Provider shall, at its sole cost and expense, keep in effect at all times during the term of this Agreement, any licenses, permits, and approvals which are legally required for Service Provider to practice his profession.

3) TIME. Service Provider shall devote such time and resources pursuant to this Agreement as may be reasonably necessary for satisfactory performance of Service Provider's obligations pursuant to this Agreement.

4) SERVICE PROVIDER NOT AN AGENT. Except as City may specify in writing, Service Provider shall have no authority, express or implied, to act on behalf of City in any capacity whatsoever as an agent. Service Provider shall have no authority, express or implied, pursuant to this Agreement, to bind City to any obligation whatsoever.

5) ASSIGNMENT PROHIBITED. No party to this Agreement may assign any right or obligation pursuant to this Agreement. Any attempted or purported assignment of any right or obligation pursuant to this Agreement shall be void and of no effect. For purposes of clarity, any merger, consolidation, or reorganization involving Service Provider (regardless of whether Service Provider is a surviving or disappearing entity) will not be considered a transfer of rights, obligations, or performance under this Agreement, and Service Provider will not be obligated obtain consent from City. However, Service Provider must notify the City of any such merger, consolidation, or reorganization in accordance with the noticing provisions of Exhibit C, Section 14.

6) PERSONNEL. Service Provider shall assign only competent personnel to perform Services pursuant to this Agreement. In the event that City, in its sole discretion, at any time during the term of this Agreement, desires the removal of any person or persons assigned by Service Provider to perform Services pursuant to this Agreement, Service Provider shall remove any such person immediately upon receiving notice from City of the desire of City for the removal of such person or persons.

7) STANDARD OF PERFORMANCE. Service Provider shall perform all Services required pursuant to this Agreement. Services shall be performed in the manner and according to the standards observed by a competent practitioner of the profession in which Service Provider is engaged in the geographical area in which Service Provider practices

his profession. All products which Service Provider delivers to City pursuant to this Agreement shall be prepared in a workmanlike manner and conform to the standards of quality normally observed by a person practicing in Service Provider's profession. City shall be the sole judge as to whether the product of the Service Provider is satisfactory.

8) CANCELLATION OF AGREEMENT. Either Party may terminate this Agreement immediately if the other is in material breach of this Agreement and such breach is not cured within thirty (30) days following non-breaching party’s written specification of the breach. Service Provider may suspend the Services or terminate this Agreement immediately in the event the Services or City’s use of the Services provided hereunder pose a security risk to the Services, Service Provider or any third party, or become illegal or contrary to any applicable law, rule, regulation, or public policy. Upon expiration or any termination of this Agreement, City shall cease all use and refrain from all further use of the Services and other Service Provider Intellectual Property. Additionally, City shall be obligated to pay, as of the effective date of such expiration or termination, all amounts due and unpaid to Service Provider under this Agreement. Unless otherwise specified, following ninety (90) days after expiration or termination of the Agreement, Service Provider may remove City Data from Service Provider Services and without City consent or notice.

a) CANCELLATION FOR NON-APPROPRIATION OF FUNDS. City represents that it has received sufficient appropriation of funds by the applicable legislature (or other appropriate governmental body) (“Governmental Appropriation”) for the first year of the term of any Order Form executed by City (the “First Year” and all such years following the First Year which are included in the term of an Order Form, the “Future Years”). If City is subject to federal, state or local law which makes City’s financial obligations under this Services Agreement contingent upon Governmental Appropriation, and if such funds are not forthcoming or are insufficient due to failure of such Governmental Appropriation, then City will have the right to terminate the then remaining portion of any Future Years under the Services Agreement at no additional cost and with no penalty by giving prior written notice documenting the lack of funding. City will provide at least thirty (30) days advance written notice of such termination. City will use reasonable efforts to ensure appropriated funds are available. It is expressly agreed that City shall not activate this non-appropriation provision for its convenience or to circumvent the requirements of this Agreement, but only as an emergency fiscal measure during a substantial fiscal crisis, which affects generally its fiscal operations. If City terminates the Services Agreement under this Section 8, City agrees not to replace the Services with functionally similar products or services for a period of one year after the termination of the Services Agreement.

9) INDEMNIFY AND HOLD HARMLESS.

a) If AGREEMENT is an agreement for design professional services subject to California Civil Code § 2782.8(a) and Service Provider is a design professional, as defined in California Civil Code § 2782.8(c)(2), to the fullest extent allowed by law, Service Provider shall hold harmless, defend and indemnify the City, its officers, agents, employees, and volunteers from and against all claims, damages, losses, and expenses including attorneys’ fees arising out of, or pertaining to, or relating to the negligence, recklessness, or willful misconduct of the Service Provider, except where caused by the active negligence, sole negligence, or willful misconduct of the City.

b) If AGREEMENT is not an agreement for design professional services subject to California Civil Code § 2782.8(a) or Service Provider is not a design professional as defined in subsection 10(a) above, to the fullest extent allowed by law, Service Provider shall indemnify, defend, and hold harmless the City, its officers, and employees from all claims, suits, or actions of every name, kind and description, brought forth on account of injuries to or death of any person or damage to personal tangible property arising from or connected with the willful misconduct, grossly negligent acts, serious errors or omissions, ultra-hazardous activities, activities giving rise to strict liability, or defects in design by Service Provider or any person directly or indirectly employed by or acting as agent for Service Provider in the performance of this Agreement, including the concurrent or successive passive negligence of the City, its officers, or employees.

It is understood that the duty of Service Provider to indemnify and hold harmless includes the duty to defend as set forth in Section 2778 of the California Civil Code.

Acceptance of insurance certificates and endorsements required under this Agreement does not relieve Service Provider from liability under this indemnification and hold harmless clause. This indemnification and hold harmless clause shall apply whether or not such insurance policies are determined to be applicable to any such damages or claims for damages.

Service Provider's responsibility for such defense and indemnity shall survive termination or completion of this agreement for the full period of time allowed by law.

10) PROHIBITED INTERESTS. No employee of the City shall have any direct financial interest in this agreement. This agreement shall be voidable at the option of the City if this provision is violated.

11) LOCAL EMPLOYMENT POLICY. The City desires wherever possible, to hire qualified local residents to work on city projects. Local resident is defined as a person who resides in Solano County. The City encourages an active affirmative action program on the part of its contractors, sub-contractors, and developers. When local projects require, subcontractors, contractors, consultants and developers will solicit proposals from qualified local firms where possible.

As a way of responding to the provisions of the Davis-Bacon Act and this program, contractor, consultants, and developers will be asked, to provide no more frequently than monthly, a report which lists the employee's name, job class, hours worked, salary paid, city of residence, and ethnic origin.

12) SERVICE PROVIDER NOT A PUBLIC OFFICIAL. Service Provider is not a "public official" for purposes of Government Code §§ 87200 et seq. Service Provider conducts research and arrives at his or her conclusions, advice, recommendation, or counsel independent of the control and direction of the City or any City official, other than normal contract monitoring. In addition, Service Provider possesses no authority with respect to any City decision beyond these conclusions, advice, recommendation, or counsel.

13) EMPLOYMENT DEVELOPMENT DEPARTMENT REPORTING REQUIREMENTS. When the City executes an agreement for or makes payment to Service Provider in the amount of $600 (six hundred dollars) or more in any one calendar year, Service Provider shall provide the following information to City to comply with Employment Development Department (EDD) reporting requirements:

a) Whether Service Provider is doing business as a sole proprietorship, partnership, limited liability partnership, corporation, limited liability corporation, non-profit corporation or other form of organization.

b) If Service Provider is doing business as a sole proprietorship, Service Provider shall provide the full name, address and social security number or federal tax identification number of the sole proprietor.

c) If Service Provider is doing business as other than a sole proprietorship, Service Provider shall provide Service Provider’s federal tax identification number.

14) NOTICES. All notices shall be given in writing to the following addresses or other such addresses as the parties may designate by written notice:

To City: City of Fairfield
Attn: Jeffrey Bertany
c/o Information Technology Department
1000 Webster Street
Fairfield, California 94533

To Service Provider:

GovernmentJobs.Com
Attn: Sina Dashti
2120 Park Place
Suite 100
El Segundo, CA 90245

15) GOVERNING LAW AND VENUE. This Agreement shall be governed by the laws of the State of California and, in the event of litigation, venue will be in the County of Solano.

16) PROPRIETARY AND CONFIDENTIAL INFORMATION**.** Service Provider agrees that all of the information it obtains from City constitutes City's confidential property ("Confidential Information") regardless of whether such information is pre-marked as confidential or in any other manner to indicate its confidential nature. Except as expressly authorized herein, Service Provider agrees to hold in confidence and not disclose any Confidential Information. Service Provider further agrees to establish such systems and procedures as may be reasonable to maintain City's Confidential Information. Service Provider's nondisclosure obligation shall not apply to information which Service Provider can document: (a) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (b) is or has become public knowledge through no fault of Service Provider; (c) is rightfully obtained by Service Provider from a third party without breach of any confidentiality obligation; or (d) is required to be disclosed pursuant to the order or requirement of a court, administrative agency, federal law, foreign state law, California state law, applicable regulatory authorities, or other governmental body.

17) DIVULGING OF CONFIDENTIAL OR PROPRIETARY INFORMATION**.** Should City require the services of a third party to operate, maintain or modify the product(s), nothing in this Agreement shall preclude City from doing so. City shall provide Service Provider with as much notice as practicable before utilizing or divulging any proprietary information or trade secrets so that Service Provider may coordinate and or limit the delivery of said information to the third party necessary to accomplish said operation, modification or maintenance. Any third party receiving Confidential Information, proprietary information, or trade secrets under this paragraph must agree to the same prohibition against disclosure as City.

EXHIBIT “D”

INSURANCE REQUIREMENTS

Service Provider shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder by the Service Provider, its agents, representatives, or employees.

1) MINIMUM SCOPE AND LIMITS OF INSURANCE

a) Commercial General Liability coverage (occurrence Form CG 00 01) with minimum limits of $1,000,000 per occurrence for bodily injury, personal injury, products and completed operations, and property damage. If Commercial General Liability or other form with a general aggregate limit is used, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.

b) Workers’ Compensation insurance as required by the State of California and Employers’ Liability insurance, each in the amount of $1,000,000 per accident for bodily injury or disease.

2) INDUSTRY SPECIFIC COVERAGES

The following insurance is also required.

☒ Cyber Liability Insurance in the minimum amount of $1,000,000 per occurrence

3) INSURANCE PROVISIONS

a) DEDUCTIBLES AND SELF-INSURED RETENTIONS. Any deductibles or self-insured retentions must be declared to and approved by the City. At the option of the City, either the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the City, its officers, officials, employees and volunteers; or the Service Provider shall procure a bond guaranteeing payment of losses and related investigations, claim administration and defense expenses.

b) The general liability policy is to contain, or be endorsed to contain, the following provisions:

i) The City, its officers, officials, employees are to be covered as additional insureds as respects: liability arising out of work or operations performed by or on behalf of the Service Provider; products and completed operations of the Service Provider; premises owned, occupied or used by the Service Provider; and automobiles owned, leased, hired or borrowed by the Service Provider. The coverage shall contain no special limitations on the scope of protection afforded to the City, its officers, officials, employees or volunteers.

ii) For any claims related to this project, the Service Provider's insurance coverage shall be primary insurance as respects the City, its officers, officials, and employees. Any insurance or self-insurance maintained by the City, its officers, officials, or employees shall be excess of the Service Provider's insurance and shall not contribute with it.

iii) Any failure to comply with reporting or other provisions of the policies including breaches of warranties shall not affect coverage provided to the City, its officers, officials, or employees.

iv) The Service Provider's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.

v) Each insurance policy required by this clause shall be endorsed to state that coverage shall not be suspended, voided, canceled by either party, reduced in coverage or in limits except after thirty (30) days' prior written notice by certified mail, return receipt requested, has been given to the City.

vi) The policy limits of coverage shall be made available to the full limits of the policy. The minimum limits stated above shall not serve to reduce the Service Provider's policy limits of coverage. Therefore, the requirements for coverage and limits shall be (1) the minimum coverage and limits specified in this agreement, or (2) the broader coverage and maximum limits of coverage of any insurance policy or proceeds available to the named insured, whichever is greater.

c) ACCEPTABILITY OF INSURER. Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A:VII, unless otherwise acceptable to the City.

d) VERIFICATION OF COVERAGE. CONSULTANT shall furnish the CITY with original endorsements effecting coverage required by this Exhibit D. The endorsements are to be signed by a person authorized by that insurer to bind coverage on its behalf. The endorsements are to be on forms equivalent to CG 20 10 11 85 subject to CITY approval. All insurance certificates and endorsements are to be received and approved by the CITY before work commences, these documents must be submitted electronically through the Exigis insurance system, certificates-fairfield@riskworks.com. At the request of the CITY, CONSULTANT shall provide complete copies of all required insurance policies, including endorsements effecting the coverage required by these specifications.

e) SUB-CONTRACTORS. Service Provider shall require all subcontractors to procure and maintain insurance policies subject to the requirements of Exhibit D. Failure of Service Provider to verify existence of sub-contractor's insurance shall not relieve Service Provider from any claim arising from sub-contractors work on behalf of Service Provider.

EXHIBIT "E"

MUTUAL NON-DISCLOSURE AGREEMENT

Regarding Sensitive Proprietary Infrastructure Information

This Mutual Non-Disclosure Agreement ("Agreement"), is entered into this ______day of _______________, 2024 ("Effective Date"), by and between the City of Fairfield, ("City"), a municipal corporation of the State of California, and the entity responding to City's above-referenced subject for receiving such information whose name, address, and state of incorporation, are as follows: Governmentjobs.com ("NeoGOV"), 2120 Park Pl, El Segundo, CA, a California corporation. Each party (in such capacity, "**Discloser**") may disclose or provide access to certain of its confidential or proprietary information to the other party (in such capacity, "**Recipient**") pursuant to the terms of this Agreement.

WHEREAS, the City, acting through the Information Technology Department, will disclose certain Confidential Information to potential vendors who wish to work with the City, relating to the City's network configuration and infrastructure; and

WHEREAS, each potential entity who may work with the City, at the request of the Information Technology Department must have access to such information in order to configure hardware, software, application, or network services; and

WHEREAS, in order to release this Confidential Information to potential vendors, the City requires each vendor to enter into this Agreement through its authorized representative and return it to the City as a pre-condition of receiving supplemental documents that contain Confidential Information.

NOW THEREFORE, in consideration of the above recitals and the mutual promises of the parties herein contained, it is agreed by and between the parties as follows:

1. **"Confidential Information" as used in this Agreement shall mean any and all technical and non-technical information, data, documents, records, and materials provided by or on behalf of the Discloser to the Recipient, including without limitation patent, trade secret, proprietary, and systems security-related information and information related to the current, future, and proposed services of the Discloser, in any form or medium, written or oral. Confidential Information also includes other information that is marked or otherwise identified as confidential or proprietary, or that would otherwise appear to a reasonable person to be confidential or proprietary in the context and circumstances in which the information is known or used.**

Confidential Information shall not include public records subject to disclosure under the California Public Records Act, Government code section 6250 et seq. and 7929.210.

2. The Recipient agrees that it will not make use of, disseminate, or in any way disclose the Discloser's Confidential Information to any person, firm, or business, except as necessary for the Recipient to work with the Discloser, and any purpose the Discloser has authorized or hereafter authorizes in writing. The Recipient agrees that it shall disclose Confidential Information only to those directors, officers, employees, agents, affiliates, advisors, representatives, or consultants who need to know such information and who have previously agreed, either as a condition to employment or service or in order to obtain the Confidential Information, to be bound by terms and conditions substantially similar to those of this Agreement.

3. The Recipient agrees to hold all Confidential Information of the Discloser in the strictest confidence and treat it with the same degree of care as it accords to its own Confidential Information, and the Recipient represents and warrants that it exercises reasonable care to protect its own Confidential Information.

4. The Recipient's obligations under Sections 2 and 3 with respect to any portion of the Discloser's Confidential Information shall terminate if the Recipient can document that: (a) such information was in the public domain at the time it was communicated to the Recipient by the Discloser; (b) such information entered the public domain subsequent to the time it was communicated to the Recipient through no fault of the Recipient; (c) it was in the Recipient's possession free of any obligation of confidence at the time it was communicated to the Recipient by the Discloser (as shown by the Recipient's files and records as of the time of disclosure); (d) it was rightfully communicated to the Recipient by a third party free of any obligation of confidence subsequent to the time that it was communicated to the Recipient by the Discloser; (e) it was developed by employees or agents of the Recipient independently of and without reference to any information communicated to the Recipient by the Discloser; or (f) the communication was in response to a valid order by a court or other governmental body, was otherwise required by law, or was necessary to establish the rights of either party under this Agreement (provided that the Recipient has provided the Discloser with a reasonable opportunity to seek protective legal treatment for such Confidential Information).

5. All materials (including, without limitation, documents, drawings, models, apparatus, sketches, designs, and lists) furnished to the Recipient by the Discloser shall remain the property of the Discloser and shall be returned promptly upon request, together with any copies thereof, or destroyed with the consent of the Discloser.

6. The Recipient shall not assign or transfer any rights or obligations under this Agreement without the prior written consent of the Discloser.

7. Recipient's obligations under this Agreement shall survive the termination of any other contractual agreement between the parties.

8. This Agreement shall be governed in all respects by the laws of the United States of America and by the laws of the State of California. The sole jurisdiction and venue for any dispute arising under this Agreement shall be the state and federal courts located in Solano County, CA, and each party to this Agreement hereby submits to such jurisdiction and venue.

9. This Agreement may only be changed by mutual agreement of authorized representatives of the parties in writing.

10. The Recipient acknowledges and agrees that irreparable injury may result to the Discloser if the Recipient breaches the provisions of this Agreement and that damages may be an inadequate remedy in respect of such breach. The Recipient agrees in advance that, in the event of such breach, the Discloser shall be entitled to the granting of injunctive relief in the Discloser's favor, in addition to such other remedies, damages and relief as may be available under applicable law.

11. This Agreement shall not be construed in any manner to be an obligation to enter into further contract or to reimburse the cost of any effort expended by Recipient.

12. This agreement constitutes the entire agreement of the parties with respect to the subject matter hereof. In the event of a dispute or a claim by a party to enforce its rights under this Agreement, the non-prevailing party shall pay all of the prevailing party's reasonable legal fees. This Agreement and all of the provisions hereof shall be binding upon and inure to the benefit of the parties hereto and their respective successors, transferees, and assignees.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first written above.

RECIPIENT:

By: DocuSigned by:
C48A2B32DE9F457...

Name: Alex Chun

Title: CFO

Date: 9/12/2024 | 10:10:56 AM PDT

CITY OF FAIRFIELD:

By: ______________________

Name: ______________________

Title: ______________________

Date: