SECOND AMENDMENT TO AGREEMENT

THIS AMENDMENT is made and entered into by and between the CITY OF FRESNO, a California municipal corporation (hereinafter referred to as City), and Sherpa Government Solutions LLC, a Limited Liability Company, a subsidiary of GTY Technology Holding Inc. dba Euna Solutions (hereinafter referred to as Contractor) as follows:

RECITALS

WHEREAS, City and Contractor entered into an Agreement dated October 31, 2019, for services related to an on-premises license service (Agreement); and

WHEREAS, the City and the Contractor entered into a First Amendment on May 23, 2024, to modify the scope of work and provide additional services; and

WHEREAS, City and Contractor now desire to enter into this Second Amendment to modify the agreement to increase the scope of work necessary, for an amount of $25,000 for an initial term of two (2) years for a total contract amount of $50,000; and

WHEREAS, with entry into this Agreement, the Contractor agrees it has no claim, demand, or dispute against the City.

AGREEMENT

1. SCOPE. The City wishes to modernize their current Budget Formulation and Management (BFM) solution. The modernization will require a re-implementation of BFM software including upgrading from an on-premises license to a hosted SaaS subscription.

2. ORDER FORM. City accepts Contractor's Proposal as stated and agrees to pay the consideration stated, at the times, in the amounts, and under the conditions specified in the Contract Amendment Documents.

2.1 Hosting Fees. Hosting subscription fees will be due upon installation and annually thereafter.

Product	Description	Subscription Dates	Amount
Hosting	2 environments: (PROD and DEV)	11/1/2024 – 10/31/2025	$ 25,000.00
Hosting	2 environments: (PROD and DEV)	11/1/2025 – 10/31/2026	$ 25,000.00

2.2 Due Date. Fees for Hosting Subscription are payable annually and commencing on the Order Effective Date for Hosting Subscription.

2.3 Term. The initial term of this Order shall begin on the Order Effective Date and shall continue for two (2) years (the "Initial Term"). The Initial Term may be extended by both parties authorized representatives.

4.0 SLA. Cloud-Based Services Service Level Agreement.

SERVICE LEVEL AGREEMENT FOR CLOUD-BASED SERVICES IN A PRODUCTION ENVIRONMENT

The following section sets out the Service Level Metrics applicable to Sherpa's cloud-based Services.

Metrics in this document apply to the service level for the hosting level: ***Continental United States, Standard Availability Environment***. Vendor offers additional hosting levels with different metrics.

1. Definitions

Subscriber - The purchaser of the cloud-based services, including, without limitation, all its subdivisions, departments, and constituent entities within its legal scope and jurisdiction.

Vendor - Sherpa Government Solutions

Hosting Region - Vendor offers hosting through Amazon Web Services (AWS) in three regions:

- US-EAST-1 – Virginia
- US-EAST-2 – Ohio
- US-WEST-2 –Oregon

We locate each Subscriber closest geographically. Note that exact locations will not be provided (no addresses are available).

Day - A Day is a business day, excluding weekends and Vendor holidays.

Business Hours - Defined as 6:00am to 6:00pm Pacific Standard Time, Monday to Friday.

Hour - An Hour is defined as an hour within Business Hours. For example, if an incident is reported on Monday, 6:00pm PST with a 4 hour response time, the incident response period is from Monday, 6:00pm PST to Tuesday,11:00am PST. During critical Subscriber budget development times, Vendor will make commercially reasonable efforts to extend support outside of Business Hours.

1.1. Incident Definition

Incident(s) - Is an event that is not part of normal operations that disrupts an operational process or processes. An incident may involve the failure of a feature or service that should have been delivered or other type of operation failure.

1.2. Incident Priority Level Definitions

Tier 1 Incidents - Tier 1 incidents have a major impact on the Subscriber's ability to operate their entire business processes. No work-around or manual process is available.

Tier 2 Incidents - Tier 2 incidents include system or component failure or malfunction causing impact on Subscriber's ability to operate significant business processes. A work-around or manual process may be available but is not a viable option for continued business operations.

Tier 3 Incidents - Tier 3 incidents include component failure or malfunction not causing impact on Subscriber's ability to operate significant business processes. Work-around or manual processes are available.

Tier 4 Incidents - Low level incidents are cosmetic or 'nice to have' requests that have minimal impact on business processes. These will be prioritized and included in the standard release schedule when possible. No communication standard is assigned for this incident tier.

1.3. Support Requests

Support Requests - Subscriber's support requests not relating to an incident will be responded to promptly. Start work and resolution times are dependent on the nature of the request. Support Requests do not have Service Metrics applied.

2. Incident Response

The Vendor will communicate with the Subscriber throughout the resolution period for Tier 1 and Tier 2 Incidents, ensuring that the Subscriber is aware of the estimated Resolution Time, and if they expect the resolution to exceed the Target Resolution Time. The Vendor will make commercially reasonable efforts to resolve Tier 1 and Tier 2 within the respective Resolution Time Targets.

The following standards apply to the response to and handling of incidents impacting customers.

Incident Priority Level		**Tier 1**	**Tier 2**	**Tier 3**	**Support Requests**
Response Within	Initial Response	1 hour	1 hour	4 hours	4 hours
	Start Work	2 hours	4 hours	8 hours	8 hours
	Resolution	4 hours	8 hours	4 days	4 days
Compliance Target		100%	100%	100%	100%
Communication Methods		• Email to the Subscriber primary contact acknowledging the incident and process to resolve. • Phone or email for follow-up communication. • Communication through our Customer Support / ticketing system.			

Vendor will provide Resolutions with the least disruption to business operations possible. This may be comprised of interim workarounds, 'hot-fix' changes, which do not require a

software upgrade, or code changes that do require a software upgrade. Before applying any changes that would result in a software upgrade, Vendor will notify the Subscriber prior to proceeding and obtain approval. If a Subscriber selects to not receive the Resolution for any reason or wishes to delay the Resolution until a later date, the Incident is considered resolved for purposes of Service Metrics.
date, the Incident is considered resolved for purposes of Service Metrics.

3. Notifications

3.1. Event Notification

The following standards apply to notification of events that have happened or will happen.

Level	**Planned A**	**Planned B**	**Planned C**	**Unplanned A**
Response	1 week prior	3 days prior	1 day prior	3 days after
Compliance Target	100%	100%	100%	100%
Communication Methods	• Email to the Subscriber primary contact notifying of the event. • Phone available for follow up communication.			

3.2. Notifications – Planned Events

Vendor will provide notification of planned maintenance and service depending on the impact to the customer and the duration of impact.

Maintenance Type	**Communication Standard**
Planned emergency outage.	Event Notification - Planned C
Planned emergency maintenance including but not limited to urgent patches.	Event Notification - Planned C
Regular maintenance (requiring downtime) including but not limited to defect fixes, software patches and hardware maintenance. Downtime of 4 hours or less, outside of business hours.	Event Notification - Planned B
Regular maintenance (requiring downtime) including but not limited to software upgrades, defect fixes, software patches and hardware maintenance. Downtime of more than 4 hours.	Event Notification - Planned A

3.3. Notifications – Unplanned Events

Vendor may need to communicate events to Subscriber that were not planned. Such events may include, but are not limited to, the following:

- Emergency maintenance
- Internet/network outages beyond Vendor's control affecting the Vendor application
- Unplanned service degradation
- Natural Disasters affecting the Vendor application

Communication Standard: ***Event Notification Unplanned A***

4. After Hours Support

After hours support can be requested by the Subscriber. Vendor requires 48 hours notice to allow for scheduling of after-hours support. If advanced notice is not given, Vendor will make commercially reasonable efforts to provide the requisite support.

5. Submitting Incidents

Subscribers must submit tickets through Vendor's customer success system to ensure incident metrics are tracked properly. Tickets should include, where relevant:

- Environment impacted
- User ID used to create the incident
- Steps to recreate
- Screen shots of the issue
- Business impact

6. Service Metrics

6.1. Availability

Metric: Availability ≥ 99.72%

Measurement Period: Monthly

Measurement: Availability with respect to any cloud-based Service in any month equals the number of uptime minutes divided by the number of minutes in the month and multiplied by 100, e.g., a 30 day month will have 43,200 total minutes (30 days x 24 hours x 60 minutes) so if total downtime were 120 min, the Availability would be 99.72% (43,080/43,200 x 100).

Downtime with respect to any month equals the sum of all periods of time during that month when any of the following events are occurring other than as a result of Scheduled Maintenance: (i) the cloud-based Service cannot be accessed by any User; (ii) the performance of the cloud-base Service is materially compromised; or (iii) the Subscriber is unable to use the cloud-based Service to access the Subscriber Data; (iv) a critical function with the cloud-based service is unavailable or is materially compromised.

Scheduled Maintenance means any maintenance conducted by Vendor:

(i) Between 12:00 a.m. and 7:00 a.m. (local server time) or (ii) during any maintenance period for which the Subscriber has been given written notice at least three (3) Business Days in advance of the first day of the maintenance period (provided that the maintenance period does not last longer than 24-hours in total).

(ii) In rare cases, emergency maintenance may be required with little notice.

6.2. Restore Time

Metric: No single period of Down Time will last longer than four (4) hours.

Measurement Period: Each incident

Measurement: A period of Down Time begins at the earlier of the following times: (i) when Vendor becomes aware of the outage or partial outage through its own monitoring efforts; and (ii) when any one of the Vendor's clients reports the outage to Vendor.

A period of Down Time ends when: (i) the cloud-based Service is functioning in substantial accordance with its specifications; and (ii) the Subscriber confirms that it is able to access the affected cloud-based Service and use the cloud-based Service to access the Subscriber Data.

6.3. Incident Response

Metric: Incident Response Time Targets Met 100%

Measurement Period: Monthly

Measurement: Incident Response Time starts at the time an incident is reported by the Subscriber during regular business hours via the Vendor's incident reporting system.

Incident Response Time ends when: (i) the Vendor starts work on the ticket; and (ii) when the Vendor acknowledges receipt of the ticket.

6.4. Incident Resolution

Metric: Incident Resolution Time Targets Met ≥ 99%

Measurement Period: Monthly

Measurement: Incident Resolution Time starts at the time an incident is reported by the Subscriber via the Vendor's incident reporting system.

Incident Resolution Time ends when: (i) a solution has been provided and implemented that resolves the reported incident; or (ii) a work-a-round acceptable to the Subscriber is provided that provides a temporary solution to the reported incident; or (iii) a time frame for implementation of the solution to the reported incident has been established that is acceptable to the Subscriber.

6.5. Disaster Recovery

Metric: Disaster Recovery Target Met

Measurement Period: Any Disaster Event

Measurement: If there is a disaster, the application will be recovered within twenty-four (24) clock hours. For example, if a disaster is reported at 1:00pm on Monday, it will be recovered by 1:00pm on the next day, Tuesday. Disaster Recovery Time starts when a disaster event is encountered that critically impacts the application. Disaster Recovery Time ends when services have been restored.

6.6. Request for Support made within defined Business Hours

Metric: Response time for Request for Support made within defined Business Hours

Measurement Period: Quarterly

Measurement: The average time to return any request for support is four hours.

6.7. RPO, RTO and Backup

Logs are exported from 6am to 6pm local server time on a 30-minute cycle. Vendor operates with a Recovery Point Objective (RPO) during Business Hours of 30 minutes. Vendor Recovery Time Objective (RTO) during Business Hours is 4 hours. The RTO outside of Business Hours is 16 hours.

Vendor will be partnering with AWS and utilizing a data center closest to each customer. All data being transferred between the customer's network and the AWS hosting site would be handled through encrypted channels.

The proposed solution/pricing for this hosting level does not include clustering for hot fail-over.

- With a major system failure, Vendor can restore to the last backup/log, which is in 30 minute increments.
- Vendor can recover 7 days up to the minute from the last backup point
- Full Nightly backups are taken at midnight. This means Vendor can provide restore points to the minute by taking log files up to the 30 minute log file period and restore to the minute required (e.g., provide a backup from 5 days ago at 9:23 am; log files are selected through 9:30am and restore process will restore data to the 9:23am mark).
- Vendor has a full system backup every Sunday that goes back 1 month
- Vendor has a monthly backup that goes back 12 months.

All servers and databases are snapshot nightly and stored for 14 days.

Currently Vendor backups all databases and SFTP file transfers to the AWS S3 storage. This is a fully redundant backup system across multiple zones/regions so recovery can be done from these sources in the case of catastrophic failure at any individual AWS data center. The Snapshots are housed within the S3 environment which means snapshots can be recovered at any time.

In the event of corrupted data on the database server, the most recent uncorrupted snapshot will be restored to a new server. In most cases, data can be recovered to as little as 30 minutes prior to the corruption. Vendor can then create a backup of the restored database and refresh the corrupted database on the primary database server. In most cases the process takes a few hours. Larger databases will take longer to restore than smaller databases. In the absolute worst-case scenario, where the data center is no longer allowing RDS service, Vendor can switch to a region that has the RDS service running and bring a database online in that region from the most recent uncorrupted source.

6.8. Disaster Recovery and Business Continuity

See Vendor's ***Disaster Recovery*** and ***Business Continuity*** documents for additional detail.

7. Other Services

The Vendor shall demonstrate compliance to support the implemented Vendor software through:

- Continued investment and development of the budget application
- Management of ongoing updates
- Management of tickets and resolution
- Management of approved changes and enhancements

8. Enhancement Requests

Enhancement requests are Subscriber requests that will alter the software as currently designed, by adding functionality or changing existing functionality. Enhancement Requests are not included in Service Metrics.

The Vendor Product Manager, with the support of the Technical Manager, approves all new functionality. In some cases, enhancement requests may be modified to make the request configurable and usable by multiple Subscribers. Requesting Subscribers may review these modifications prior to the beginning of development.

Enhancement Requests can be made directly in the Vendor's customer success / ticketing system, or if applicable, can be submitted to the implementation team directly.

Small Enhancement: If the change request is low impact, then the change may be made immediately, typically within a week. If the change is high impact, then Vendor will work with the Subscriber to schedule it at the appropriate time. High impact is typically defined as requiring a software upgrade or significant regression testing.

Medium Enhancement: Vendor will follow the same procedure as Small Change, but the target time to complete the change is 1-3 weeks.

Large Enhancement: There are two categories of large changes. Categorization of the change is solely determined by Subscriber's Product manager. The categories defined as such:

1. If the change is applicable to both the requesting Subscriber and would likely be used by other Subscribers, or the lack of this functionality is a software deficiency, this change request will be added to Vendor's current development schedule.
2. If the change is Subscriber-specific, then Vendor will estimate the cost (if any) for the system change and discuss implementation options with the Subscriber.

Enhancements During Implementation: Subscribers will be receiving upgrades on a regular basis throughout the implementation (often weekly) until go-live preparation begins. This allows enhancements or any new features to be included in the software as they become available. Enhancements will thus be available regardless of if a software upgrade is required.

9. Software Upgrades

Vendor software is updated on a regular basis and is deployed to Subscribers based on a schedule agreed to by the Vendor and Subscriber. Vendor will not apply upgrades to a Production environment without prior notice to the Subscriber. A typical schedule for upgrades is once annually in the period between budget adoption and the subsequent budget cycle start.

Vendor will request a planned system outage to allow for proper testing once upgrades are applied to production. Typical planned system outage is one day; the system is available during this period but Vendor requests minimal activity in the system to allow for efficient testing.

9.1. Vendor Responsibilities

- Copy Production to Development and make appropriate backups
- Apply upgrades
- Unit test software in the client environment, including non-impactful testing in Production (no data is impacted)

9.2. Subscriber Responsibilities

- Approve the upgrade schedule at least 30 days in advance of the upgrade date
- Subscriber testing is not required. If the Subscriber wishes to participate in upgrade testing, it is allowed.

10. Security Incident Response

10.1. Overview

Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Vendor has implemented a wide variety of preventive, investigative, and corrective security controls with the objective of protecting information assets.

Ultimately to manage any incident such that recovery time and costs are limited, as well as taking commercially reasonable steps possible to ensure an improved security stance.

10.2. Network Protection

Vendor's network protections include solutions designed to provide continuity of service, defending against Distributed Denial of Service (DDoS) attacks.

10.3. Monitoring and Event Alerts

Alerts are sent to Vendor's security team for review and response to potential threats. These alerts are monitored 24x7x365.

10.4. Security Incident Response

Vendor evaluates and responds to suspicious activity/events of unauthorized access to or handling of customer data, whether the data is held in Vendor's hosting environment within AWS or on personal hardware assets of Vendor employees. Vendor's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes the Vendor security team to serve as the primary

contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution.
Vendor security team will:

- Validate that an incident has occurred
- Communicate with relevant stakeholders
- Preserve evidence
- Document any incident along with related response activities
- Take actions to contain an incident
- Escalate an incident as necessary
- Prevent any future re-occurrence of the incident or tangentially related security concerns

Upon discovery of an incident, Vendor defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which will improve security posture and defense in depth. Formal procedures and central systems are utilized to collect information and maintain a chain of custody for evidence during incident investigation.

10.5. Notifications
If Vendor determines that a security incident has occurred, Vendor promptly notifies any impacted Subscribers or other third parties in accordance with its contractual and regulatory responsibilities.

11. In the event of any conflict between the body of this Amendment and any Exhibit or Attachment hereto, the terms and conditions of the body of this Amendment shall control and take precedence over the terms and conditions expressed within the Exhibit or Attachment. Furthermore, any terms or conditions contained within any Exhibit or Attachment hereto which purport to modify the allocation of risk between the parties, provided for within the body of this Amendment, shall be null and void.

11.1. Except as otherwise provided herein, the Agreement entered into by City and Contractor, dated October 31, 2019, and amended on May 23, 2024, remains in full force and effect.

[Signatures follow on the next page.]

IN WITNESS WHEREOF, the parties have executed this Amendment 2 to Sherpa Budget Formulation and Management License And Service Agreement at Fresno, California, the day and year first above written.

CITY OF FRESNO,
a California municipal corporation

By: ______________________
Georgeanne A. White,
City Manager

APPROVED AS TO FORM:
ANDREW JANZ
City Attorney

DocuSigned by:
Christine Charitar 4/25/2024
By: 86080C14183B4F3...
Christine C. Charitar Date
Deputy City Attorney

ATTEST:
TODD STERMER, CMC
City Clerk

By: ______________________

Deputy

Sherpa Government Solutions, LLC

By: Dawn S. Rippentrop

Name: Dawn Rippentrop

Title: VP Sales
(If corporation or LLC., Board Chair, Pres. or Vice Pres.)

By: ______________________

Name: Brenna Lenchak

Title: Secretary
(If corporation or LLC., CFO, Treasurer, Secretary or Assistant Secretary)

Any Applicable Professional License:
Number: ______________________
Name: ______________________
Date of Issuance: ______________________

CITY:
City of Fresno
Attention: Henry J. Fierro Budget Director
2600 Fresno Street
Fresno, CA 93721
E-mail: henry.fierro@fresno.gov

CONSULTANT:
Sherpa Government Solutions, LLC
2990 Osceola Street
Denver, CO 80212
Phone: 913-221-5422
E-mail:
dawn.rippentrop@eunasolutions.com

Attachment:

- Exhibit A Insurance Requirements and Indemnification

Exhibit A

INSURANCE REQUIREMENTS AND INDEMNIFICATION

INDEMNIFICATION

To the furthest extent allowed by law, CONTRACTOR shall defend, indemnify and hold harmless City, its officers, officials, employees, agents and volunteers (the "City Parties") from and against any and all direct and indirect claims, losses, liabilities, damages, costs and expenses (including losses and costs incurred by City, and any reasonable attorney's fees and costs) incurred by City Parties resulting from any third-party claim which arise from CONTRACTOR's negligence or willful misconduct; a breach of CONTRACTOR's confidentiality (information not of public record) obligations arising from CONTRACTOR's negligence or willful misconduct; or CONTRACTOR's violation of a law applicable to CONTRACTOR's performance under the contract. City will notify CONTRACTOR promptly in writing of the claim and give CONTRACTOR control over its defense or settlement with City's approval, reasonable approval will not be withheld. City agrees to provide CONTRACTOR with reasonable assistance, cooperation, and information in defending the claim at CONTRACTOR's expense.

If CONTRACTOR subcontracts all or any portion of the services to be performed under this Agreement, CONTRACTOR will require each subcontractor to indemnify, hold harmless and defend City and your officers, officials, employees, agents and volunteers in accordance with this paragraph.

This section shall survive termination or expiration of this Agreement.

INSURANCE REQUIREMENTS

(a) Throughout the life of this Agreement, CONTRACTOR shall pay for and maintain in full force and effect all insurance as required herein with an insurance company(ies) either (i) admitted by the California Insurance Commissioner to do business in the State of California and rated no less than "A-VII" in the Best's Insurance Rating Guide, or (ii) as may be authorized in writing by CITY'S Risk Manager or his/her designee at any time and in his/her sole discretion. The required policies of insurance as stated herein shall maintain limits of liability of not less than those amounts stated therein. However, the insurance limits available to CITY, its officers, officials, employees, agents and volunteers as additional insureds, shall be the greater of the minimum limits specified therein or the full limit of any insurance proceeds to the named insured.

(b) If at any time during the life of the Agreement or any extension, CONTRACTOR or any of its subcontractors fail to maintain any required insurance in full force and effect, all services and work under this Agreement shall be discontinued immediately, and all payments due or that become due to CONTRACTOR shall be withheld until notice is received by CITY that the required insurance has been restored to full force and effect and that the premiums therefore have been paid for a period satisfactory to CITY. Any failure to maintain the required insurance shall be sufficient cause for CITY to terminate this Agreement. No action taken by CITY pursuant to this section shall in any way relieve CONTRACTOR of its responsibilities under this Agreement. The phrase "fail to maintain any required insurance" shall include, without limitation, notification received by CITY that an insurer has commenced proceedings, or has had proceedings commenced against it, indicating that the insurer is insolvent.

(c) The fact that insurance is obtained by CONTRACTOR shall not be deemed to release or diminish the liability of CONTRACTOR, including, without limitation, liability under the indemnity provisions of this Agreement. The duty to indemnify CITY shall apply to all claims and liability regardless of whether any insurance policies are applicable. The policy limits do not act as a limitation upon the amount of indemnification to be provided by CONTRACTOR. Approval or purchase of any insurance contracts or policies shall in no way relieve from liability nor limit the liability of CONTRACTOR, vendors, suppliers, invitees, contractors, sub-contractors, subcontractors, or anyone employed directly or indirectly by any of them.

Coverage shall be at least as broad as:

1. The most current version of Insurance Services Office (ISO) Commercial General Liability Coverage Form CG 00 01, providing liability coverage arising out of your business operations. The Commercial General Liability policy shall be written on an occurrence form and shall provide coverage for "bodily injury," "property damage" and "personal and advertising injury" with coverage for premises and operations (including the use of owned and non-owned equipment), products and completed operations, and contractual liability (including, without limitation, indemnity obligations under the Agreement) with limits of liability not less than those set forth under "Minimum Limits of Insurance."

2. The most current version of ISO *Commercial Auto Coverage Form CA 00 01, providing liability coverage arising out of the ownership, maintenance or use of automobiles in the course of your business operations. The Automobile Policy shall be written on an occurrence form and shall provide coverage for all owned, hired, and non-owned automobiles or other licensed vehicles (Code 1- Any Auto).

3. Workers' Compensation insurance as required by the State of California and Employer's Liability Insurance.

4. Cyber Liability (Privacy and Data breach) insurance appropriate to CONTRACTOR'S profession.

MINIMUM LIMITS OF INSURANCE

CONTRACTOR, or any party the CONTRACTOR subcontracts with, shall maintain limits of liability of not less than those set forth below. However, insurance limits available to CITY, its officers, officials, employees, agents and volunteers as additional insureds, shall be the greater of the minimum limits specified herein or the full limit of any insurance proceeds available to the named insured:

1. COMMERCIAL GENERAL LIABILITY:

(i) $1,000,000 per occurrence for bodily injury and property damage;

(ii) $1,000,000 per occurrence for personal and advertising injury;

(iii) $2,000,000 aggregate for products and completed operations; and,

(iv) $2,000,000 general aggregate applying separately to the work performed under the Agreement.

2. To the extent that Contractor performs on-site services, COMMERCIAL AUTOMOBILE LIABILITY:

$1,000,000 per accident for bodily injury and property damage.

3. To the extent that Contractor performs on-site services, WORKERS' COMPENSATION INSURANCE as required by the State of California with statutory limits.

4. EMPLOYER'S LIABILITY:
(i) $1,000,000 each accident for bodily injury;
(ii) $1,000,000 disease each employee; and,
(iii) $1,000,000 disease policy limit.

5. CYBER LIABILITY insurance with limits of not less than:
(i) $1,000,000 per claim/occurrence; and,
(ii) $2,000,000 policy aggregate

UMBRELLA OR EXCESS INSURANCE

In the event CONTRACTOR purchases an Umbrella or Excess insurance policy(ies) to meet the "Minimum Limits of Insurance," this insurance policy(ies) shall "follow form" and afford no less coverage than the primary insurance policy(ies). In addition, such Umbrella or Excess insurance policy(ies) shall also apply on a primary and non-contributory basis for the benefit of the CITY, its officers, officials, employees, agents and volunteers.

DEDUCTIBLES AND SELF-INSURED RETENTIONS

CONTRACTOR shall be responsible for payment of any deductibles contained in any insurance policy(ies) required herein and CONTRACTOR shall also be responsible for payment of any self-insured retentions.

OTHER INSURANCE PROVISIONS/ENDORSEMENTS

The General Liability and Automobile Liability insurance policies are to contain, or be endorsed to contain, the following provisions:

1. CITY, its officers, officials, employees, agents and volunteers are to be covered as additional insureds. Additional Insured status under the General Liability policy shall be broad as that contained in ISO Form CG 20 10 04 13 or CG 20 26 04 13.

2. The coverage shall contain no special limitations on the scope of protection afforded to CITY, its officers, officials, employees, agents and volunteers. Any available insurance proceeds in excess of the specified minimum limits and coverage shall be available to the Additional Insured.

3. For any claims relating to this Agreement, CONTRACTOR'S insurance coverage shall be primary insurance with respect to the CITY, its officers, officials, employees, agents and volunteers. Any insurance or self-insurance maintained by the CITY, its officers, officials, employees, agents and volunteers shall be in excess of CONTRACTOR'S insurance and shall not contribute with it. CONTRACTOR shall establish primary and non-contributory status under the General Liability policy by use of ISO Form CG 20 01 04 13 or by an executed manuscript insurance company endorsement that provides primary and non contributory status as broad as that contained in ISO Form CG 20 01 04 13.

All policies of insurance shall contain, or be endorsed to contain, the following provision: CONTRACTOR and its insurer shall waive any right of subrogation against CITY, its officers, officials, employees, agents and volunteers.

Contractor shall provide the annual certificate of insurance upon request by CITY. All policies of insurance required herein shall be endorsed to provide that the coverage shall not be cancelled, non-renewed, reduced in coverage or in limits except after thirty (30) calendar days written notice by certified mail, return receipt requested, has been given to CITY. If endorsement is not available, the CONTRACTOR is responsible for providing written notice to the CITY under the same terms and conditions. Upon issuance by the insurer, broker, or agent of a notice of cancellation, non-renewal, or reduction in coverage or in limits, CONTRACTOR shall furnish CITY with a new certificate and applicable endorsements for such policy(ies). In the event any policy is due to expire during the work to be performed for CITY, CONTRACTOR shall provide a new certificate, and applicable endorsements, evidencing renewal of such policy.

The Cyber Liability insurance shall cover claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information (including credit monitoring costs), alteration of electronic information, extortion and network security. Such coverage is required for claims involving any professional services for which CONTRACTOR is engaged with the City for such length of time as necessary to cover any and all claims

If the Cyber Liability insurance policy is written on a claims-made form:

1. The retroactive date must be shown, and must be before the effective date of the Agreement or the commencement of work by CONTRACTOR.

2. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the Agreement work or termination of the Agreement, whichever occurs first, or, in the alternative, the policy shall be endorsed to provide not less than a five (5) year discovery period.

3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the Agreement or the commencement of work by CONTRACTOR, CONTRACTOR must purchase "extended reporting" coverage for a minimum of five (5) years completion of the Agreement work or termination of the Agreement, whichever occurs first.

4. A copy of the claims reporting requirements must be submitted to CITY for review.

5. These requirements shall survive expiration or termination of the Agreement.

Should any of these policies provide that the defense costs are paid within the Limits of Liability, thereby reducing the available limits by defense costs, then the requirement for the Limits of Liability of these polices will be twice the above stated limits.

The fact that insurance is obtained by CONTRACTOR shall not be deemed to release or diminish the liability of CONTRACTOR, including, without limitation, liability under the indemnity provisions of this Agreement. The policy limits do not act as a limitation upon the amount of indemnification to be provided by CONTRACTOR. Approval or purchase of any insurance contracts or policies shall in no way relieve from liability nor limit the liability of CONTRACTOR, its principals, officers, agents, employees, persons under the supervision of CONTRACTOR, vendors, suppliers, invitees, consultants, subcontractors, or anyone employed directly or indirectly by any of them.

VERIFICATION OF COVERAGE

CONTRACTOR shall furnish CITY with all certificate(s) and applicable endorsements effecting coverage required hereunder. All certificates and applicable endorsements are to be received and approved by the CITY'S Risk Manager or his/her designee prior to CITY'S execution of the Agreement and before work commences. All non-ISO endorsements amending policy coverage shall be executed by a licensed and authorized agent or broker. Upon request of CITY, CONTRACTOR shall immediately furnish City with a complete copy of any insurance policy required under this Agreement, including all endorsements, with said copy certified by the underwriter to be a true and correct copy of the original policy. This requirement shall survive expiration or termination of this Agreement.

SUBCONTRACTORS

If CONTRACTOR subcontracts any or all of the services to be performed under this Agreement, CONTRACTOR shall require, at the discretion of the CITY Risk Manager or designee, subcontractor(s) to enter into a separate Side Agreement with the City to provide required indemnification and insurance protection. Any required Side Agreement(s) and associated insurance documents for the subcontractor must be reviewed and preapproved by CITY Risk Manager or designee. If no Side Agreement is required, CONTRACTOR will be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required by applicable law and is customary in the relevant industry.

SECOND AMENDMENT TO AGREEMENT (2)

Final Audit Report 2024-04-25

Created:	2024-04-25
By:	Dominique Malogorski (Dominique.Malogorski@eunasolutions.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAUwj4I0DBWcyNMt3OvoeGI_luI5Z28VMv

"SECOND AMENDMENT TO AGREEMENT (2)" History

Document created by Dominique Malogorski (Dominique.Malogorski@eunasolutions.com)
2024-04-25 - 5:58:34 PM GMT

Document emailed to Brenna Lenchak (brenna.lenchak@eunasolutions.com) for signature
2024-04-25 - 5:59:26 PM GMT

Email viewed by Brenna Lenchak (brenna.lenchak@eunasolutions.com)
2024-04-25 - 6:08:43 PM GMT

Document e-signed by Brenna Lenchak (brenna.lenchak@eunasolutions.com)
Signature Date: 2024-04-25 - 6:08:53 PM GMT - Time Source: server

Document emailed to Dawn Rippentrop (dawn.rippentrop@eunasolutions.com) for signature
2024-04-25 - 6:08:56 PM GMT

Email viewed by Dawn Rippentrop (dawn.rippentrop@eunasolutions.com)
2024-04-25 - 6:44:42 PM GMT

Document e-signed by Dawn Rippentrop (dawn.rippentrop@eunasolutions.com)
Signature Date: 2024-04-25 - 6:44:52 PM GMT - Time Source: server

✓ Agreement completed.
2024-04-25 - 6:44:52 PM GMT