<div align="center">

OSISOFT, LLC
ENTERPRISE PROGRAM AGREEMENT AMENDMENT

AMENDMENT EFFECTIVE DATE: July 20, 2021

</div>

This is an Amendment (the *"Amendment"*) to that certain Enterprise Program Agreement with an effective date of July 20, 2016, OSIsoft Agreement # 1018185EA, (the *"Agreement"*) by and between **OSIsoft, LLC** (*"OSIsoft"*), and **City of Riverside** (*"Licensee"*). Unless otherwise specified, all capitalized terms in this Amendment have the meaning defined in the Agreement.

WHEREAS, for the payment of license and service fees for additional Licensed Assets, to be received by OSIsoft in accordance with the Commercial Terms set forth below, the Parties wish to amend their Agreement as follows:

1. **Section 1** of the Agreement is replaced in its entirety as of the Effective Date of this Amendment with the following:

1. COMMERCIAL TERMS

Renewal Period	July 20, 2021 through August 14, 2026
Enterprise Licensed Software	• Enterprise Infrastructure Version 2.0 as further described on **Attachment 1** to the Agreement, and updated at OSIsoft.com (currently, **https://www.osisoft.com/terms-and-conditions/enterprise-agreement-software-services).** • PI Integrator for Esri ArcGIS • PI Integrator for Business Analytics – BI Edition
Annual Enterprise Services Fee ("ESRP")	Licensee's first year Enterprise Services subscription rate of this Renewal Period shall be equal to 20% (*"Enterprise Services Rate"*) of the License Fee Basis and shall increase by 5% year-on-year thereafter during the Renewal Period until the Agreement expires or terminates. *"License Fee Basis"* shall be the Initial License Fee paid under this Agreement during its Initial Term, plus any additional license fees paid hereunder for Enterprise Licensed Software's use with additional Assets or Capacity.
Initial License Fee	Licensee shall receive Enterprise Licensed Software for the Assets specified in **Exhibit A** (*"Licensed Assets"*) for license fees paid to date for currently licensed assets, of **$1,125,134**plus any additional License fees paid for new Assets or Capacity during this Renewal Period.

Net Initial Enterprise Services Fee (ESRP) Due for period July 20, 2021 through August 14, 2022:	$240,439
ESRP in remaining Renewal Period license years (estimated)*:	4 annual payments due at beginning of each subsequent license year of this Renewal Period: * Due August 15, 2022: $227,027 August 15, 2023: $236,278 August 15, 2024: $248,092 August 15, 2025: $260,497
Initial Invoice Total	$240,439

----

* The ESRP in license years 2,3,4 and 5 respectively, will change due to any material change in the licensed assets or their capacity. See Section 4.1 of the Agreement for details.

2. In **Section 2.1** of the **Enterprise Agreement** captioned **Remote Monitoring of PI Systems ("Remote Monitoring")** the first sentence is replaced with the following:

   "Licensee will permit OSIsoft to remotely monitor certain performance metrics of Licensee's Enterprise Licensed Software *thru attended access only* (as further described in **Attachment 2** - **Enterprise Remote Monitoring Services**), in accordance with the mutually agreed Enterprise Roadmap. The parties agree that Cisco Webex® ** is the mutually acceptable method for secure screen sharing and other communications in which Licensee requires OSIsoft's secure access to Licensee's information, and that Licensee will initiate and close all such communications requiring such access." (** Each party is responsible independently of each other, for securing the proper license to use the Webex tool for this purpose.)

3. In **Section 2.3** of the **Enterprise Agreement** and subsequently, replace all references to **"Enterprise Service Manager"** and **"EPM,"** with **"Customer Success Manager"** and **"CSM."**

4. In **Section 2.6** of the **Enterprise Agreement** the following is added to the end of such Section 2.6: "The installation under this Section 2.6 excludes Remote Monitoring by OSIsoft."

5. **Section 2.7** of the **Enterprise Agreement** is replaced in its entirety with the following:

   OSIsoft will provide Licensee with reasonable assistance and information resources in Licensee's application of Enterprise Infrastructure for Licensee's particular needs, per the initiatives jointly agreed upon in the annual Enterprise Roadmap.

   The scope of work for each Technical Advisory Service engagement will be created by the CSM for Licensee's review and approval. The scope of work will include a description of the deliverables, Licensee's required participation, applicable costs, if any, and the anticipated scheduling. Licensee shall bear complete responsibility for determining whether any concepts, preliminary designs, application recommendations or advice OSIsoft provide Licensee is

appropriate for Licensee's operations. OSIsoft's personnel delivering Technical Advisory Services will strive to understand Licensee's business, but in no event does OSIsoft represent that such personnel are experts in Licensee's particular industry. While Licensee's operational and business data will remain Licensee's confidential information, Licensee acknowledges that OSIsoft may utilize deliverables of general applicability which do not include Licensee's confidential information, to assist other customers or improve the Enterprise Licensed Software, even if such deliverables are based upon requirements that Licensee provides us. These materials may include, but are not limited to, non-confidential application designs, architecture, general engineering or programming methodologies in common use or within a particular industry, algorithms, sample screens or enhancements to the Enterprise Licensed Software.

6. **Section 2.09** of the **Enterprise Agreement** is replaced in its entirety with the following:

   2.09 Vouchers. Licensee will receive two different types of vouchers:

   (i) <u>Learning Vouchers</u>: Licensee will receive one (1) learning voucher per $5,000 USD paid to OSIsoft for Enterprise Services per year. These vouchers may be used for standard training courses at OSIsoft's training locations at a rate of one (1) voucher per one (1) seat per training day. Licensee may request that a standard or custom training course be conducted onsite at one of Licensee's facilities. Twelve (12) learning vouchers are required for onsite training, per day, regardless of the number of students. Onsite training is limited to a maximum of twelve (12) students per day. An additional six (6) learning vouchers (not per day; in total) will be required for a custom training course, to cover OSIsoft's additional preparation time.

   (ii) <u>Event Vouchers</u>: These vouchers may only be redeemed for admission to one of OSIsoft's user's events at a rate of one (1) seat per $40,000 USD paid to OSIsoft for Enterprise Services per year.
   From time-to-time OSIsoft may make other services or admission to other events available for purchase with these vouchers. Vouchers are valid for one (1) year from each anniversary date of the Effective Date of this enterprise agreement and cannot be carried over to subsequent years. In no event may vouchers be redeemed for anything other than the foregoing including, without limitation, software products, professional services, or cash, unless otherwise expressly agreed by Licensee and OSIsoft. Vouchers cannot be sold, bartered, swapped, or exchanged.

7. **Section 2.11** of the **Enterprise Agreement** is replaced in its entirety with the following:

   2.11. Technical Prerequisites ("Technical Prerequisites") In order for OSIsoft to provide Enterprise Services, in addition to meeting the conditions for SRP, Licensee recognizes that certain other technical pre-requisites must be met. OSIsoft will notify Licensee of such Technical Prerequisites in the Enterprise Licensed Software documentation or the Enterprise Roadmap. These prerequisites may include Licensee's acquisition of one or more additional computer servers for the Installation Management System, and Licensee access to a voice line in proximity to a relevant computer system during telephone support calls. Licensee recognizes that proper operation of Installation Management System will require installation of certain software that will be removed should Enterprise Services be terminated. Should Licensee not meet the Technical Prerequisites or otherwise prevent operation of the Installation Management System, then Remote Installation Services will not be provided.

8. The first paragraph only of **Section 4.2** of the Agreement is replaced in its entirety with the following paragraph:

> **4.2. Agreement Term.** This Enterprise Agreement will remain in effect from the Effective Date through August 14, 2026 (the **"*Renewal Period*"**). OSIsoft shall not be able to terminate this Agreement during the Renewal Period or any Renewal Period thereafter except due to Licensee's material breach of this Agreement that is not cured within 30-days' written notice from OSIsoft of such breach or due to Licensee not renewing its Enterprise Services subscription during such periods. OSIsoft will have the right to terminate this Agreement prior to any Renewal Period for any or no reason by providing notice of its intent at least one hundred eighty (180) days prior to the end of the Renewal Period or any anniversary of the Effective Date thereafter. Following this Renewal Period, for so long as Licensee, at its option, renews its Enterprise Services subscription, indicating its intent to renew, and OSIsoft does not terminate this Agreement as stated above, the Agreement will renew for successive one-year terms. In the event of termination or expiration in accordance with this section, the Enterprise Conversion Procedure in subsection 4.2(b) shall apply.

9. **Attachment 2** of the Enterprise Agreement is replaced in its entirety with **Attachment 2**, attached to and incorporated in this Amendment.

All of the terms and conditions of the Agreement shall continue in full force and effect except as modified by the terms of this Amendment. In the event of any inconsistency between the terms and conditions of this Amendment and the terms and conditions of the Agreement, the terms and conditions of this Amendment shall control and govern.

IN WITNESS WHEREOF, the parties have entered into this Amendment:

OSIsoft, LLC   **LICENSEE: City of Riverside, California**

By (sign): *Robert Guilbault*   By (sign): _____
           —DocuSigned by:
           —26A3CC74B02B44F...

Name: __Robert Guilbault__   Name: _____

Title: __EVP, Operations__   Title: _____

Date: __4/26/2021__   Date: _____

Approved as to form   Certified as to Availability of Funds:

Senior Deputy City Attorney   By: _____
                                          Chief Financial Officer

Attachment 2

Enterprise Remote Monitoring Services

Overview

These terms and conditions of service set forth the expectations of OSIsoft and the Enterprise Services system customer, associated with Critical and Standard incidents. It identifies and explains expected response times, timing of incident notifications, available remote access methods, and remedies for deficient performance of the responsibilities of OSIsoft and the customer associated with these incidents.

The applicability of these terms and conditions of service are contingent upon mutual acceptance of Site Survey Content as prepared by the Customer Success Manager and Customer.

- Remedies for deficient service level performance shall be by attended remote access only, as described below.

1. Incident Severity Levels
The incidents are identified via one of two severity levels.

Critical	The customer's PI System experiences one of the following conditions:
	    Interfaces Not Running
	    PI Server Not Running
	    PI Notifications Not Functioning Properly
	    Incident with most serious business critical impact requiring urgent resolution

Standard	The customer's PI System Experiences One Of The following conditions:
	
	    System Function Is Impaired
	    Data Collection Interruption Due To 3rd Party System Failure
	    Configuration
	    System Performance Issues
	        Application Incident with significant business critical impact requiring resolution
	        Application Incident with moderate business critical impact
	    Non-business critical application incident
	    Cosmetic requests

Incident Severity Level Descriptions

Critical Incidents
Interfaces Not Running – This indicates that data collection is compromised which may result in irreversible data loss.
PI Server Not Running – This indicates that data is currently unavailable to users and real-time data analysis. Though this does not typically indicate data loss, business operations may be affected.

Standard Incidents
System Function Is Impaired – This describes issues external to PI which are currently or will soon cause deviation from normal operation. Includes scenarios such as network or communication issues, conflicts arising from antivirus settings or operating system patching, or a lack of system resources such as critically low disk space.

Data Collection Interruption Due To 3rd Party System Failure – This indicates that the PI System is functioning normally but is unable to communicate or otherwise function normally due to 3rd party software malfunction or connectivity issue. Primarily refers to data sources such as OPC Servers, Relational Database Servers, etc.

Configuration – This indicates that a configuration in the PI System prohibits PI from running in an optimal way.

System Performance Issues – This indicates consistent issues with system components such as high memory usage, high CPU usage, or faulty hardware.

2. Incident Response Time and Notification
The Incident Response Time and Notification associated with each Severity Level is described below. The specific contact person(s) and contact method for each site will be identified by the customer via the OSIsoft Rollout Plan and Site Survey that is completed by the customer for each site. The Site Survey also identifies the remote access method (if applicable) OSIsoft support personnel utilize to access the customer's server(s).

Critical
For Critical incidents, the following response expectations apply:
> All Critical issues of which OSIsoft is notified by the customer will be reported by OSIsoft personnel via the OSIsoft Support Case Tracking System, and by telephone to the customer-specified contacts within one hour of when OSIsoft is first notified of the incident by the customer. (See below for further details on OSIsoft's standard notification process.)
> The customer may report any Critical issue by any of the following methods:
> > o By telephone (General OSIsoft support number: +1 (510) 297-5828)
> > o By submitting a Case to the OSIsoft Support Case Tracking System

(see my.osisoft.com for this and all methods of customer support through the OSIsoft Customer Portal
- o Response to a customer-initiated call will be handled by a support engineer within 1 hour after receiving the communication and an incident resolution process will be immediately initiated.
- o Incidents should be identified and documented by the customer in either a phone message or Case as a "Critical PI System Event", and otherwise must be described so that OSIsoft support personnel can reasonably identify the issue as being critical.

An incident resolution process will begin following notification.

Problem remediation will be delayed until at such time that the primary or backup customer contact can establish an attended remote access session.

If no remote access is available, incident remediation efforts will not begin until a response has been received back from the customer.

If a resolution is not accomplished within 2 hours after the start of the problem remediation, the problem may be escalated to the next level of support, or earlier if deemed necessary by OSIsoft. Escalated response "beyond critical" may include, but is not be limited to, immediate attention of higher levels of OSIsoft management and OSIsoft Product engineers to the issue, more frequent updates on problem status to the customer (usually on an hourly basis), option of prompt on-site visits, etc.

Diligent efforts towards resolution will continue by both parties until the incident is resolved.

The following notification process will be enacted for any Critical incident:

1) Upon being notified by the customer of a critical condition, OSIsoft support personnel will promptly attempt to contact the customer's Primary site contact as identified in the Site Survey.
   a. A phone call will be placed to the primary site contact.
   b. A response to the Case will be sent identifying the critical incident.
      i. The subject of the Case will begin with a short description of the event.
      ii. The body of the Case will contain relevant information regarding the critical incident.

Standard

For Standard incidents, the following response expectations apply:

All Standard issues will be reported via Case or phone to the customer-specified primary site contact within four (4) hours of when the customer first notifies OSIsoft support of the standard incident. The customer may report any Standard incident directly:
- o By telephone (General OSIsoft support number: +1 (510) 297-5828)
- o By submitting a Case to the OSIsoft Support Case Tracking System
- o Response to either a customer-initiated call or Case will be handled by a support engineer within 4 hours after receiving the

communication and an incident resolution process will be initiated. Problem remediation will be delayed until such time as the primary or backup customer contact can establish and notify OSIsoft of the availability of an attended remote access session.

If no remote access is available, incident remediation efforts will not begin until a response has been received back from the customer.

Once initiated, efforts will continue until the incident is resolved, or it is determined that the resolution is caused by 3rd party system failure, or both parties agree to suspend or discontinue resolution action.

4. Incident Tracking

Critical incidents are addressed before Standard incidents. All incidents received will result in a case being opened by the OSIsoft support Engineer via the OSIsoft Support Case Tracking System. The customer can review the details of the specific case number via the Customer's OSIsoft Customer Portal.

5. Remote Access

The following section lists the preferred network remote access method for OSIsoft support Engineers to access a customer's environment. Any deviations from these methods will need to be identified and approved in writing by OSIsoft.

Tier Criteria	Remote Access Solution
Customer does not allow unsolicited remote access but does allow solicited remote support sessions. No user accounts are provided to OSIsoft and customer requires supervision of OSIsoft sessions.	Use the OSIsoft Remote Access tool for solicited support.

Attended Remote Access

OSIsoft supports one method of attended remote access via its hosted third-party remote access solution, BeyondTrust™.

6. Performance Metrics Review

At each Enterprise Services Review Meeting, which occurs once a quarter, the following metrics will be reported upon and reviewed between the OSIsoft Enterprise Project Manager and Customer Contract Manager.

- Summary of Critical and Standard Incidents

- Detailed Review of Any Critical Incidents That Failed to Achieve Proper Response Time