STATE OF TEXAS §
§
COUNTY OF FORT BEND §

SECOND AMENDMENT TO ADDENDUM TO CONTINUANT, INC.'S AGREEMENT FOR MAINTENANCE ADVANTAGE PLAN SERVICES FY 2022

THIS SECOND AMENDMENT TO ADDENDUM TO CONTINUANT, INC.'S AGREEMENT FOR MAINTENANCE ADVANTAGE SERVICE PLAN SERVICES FY 2022 (the "Second Amendment") is made and entered into by and between Fort Bend County, (hereinafter "County"), a body corporate and politic under the laws of the State of Texas, and Continuant, Inc., (hereinafter "Continuant"), a company authorized to conduct business in the State of Texas (collectively referred to as the "parties").

W I T N E S S E T H

WHEREAS, County and Continuant executed the Addendum to Continuant, Inc.'s Agreement for Maintenance Advantage Plan Services FY 2021 on or about January 14, 2021, and as amended on or about June 22, 2021 (collectively the "Agreement"), attached hereto as "Exhibit 1", and incorporated fully by reference. County and Continuant desire to amend the Agreement as set forth below:

A. **Scope of Services**. Continuant shall render additional services in accordance with Continuant's Statement of Work for the Maintenance Advantage Plan (Agreement Number: GSA #GS-35F-552AA), attached hereto as "Exhibit 2", and incorporated fully by reference.

B. **Term**. The term of this Second Amendment is effective as of October 1, 2021, and shall expire no later than September 30, 2022, unless terminated sooner pursuant to the Agreement. Neither this Second Amendment nor the Agreement shall automatically renew, but may be subsequently renewed in writing upon agreement of the parties.

C. **Limit of Appropriation**. Continuant's fees shall be calculated at the rates set forth in the attached Exhibit 2. The Maximum Compensation for the performance of services within the Scope of Services as described in Exhibit 2 is $55,866.96. In no case shall the amount paid by County under this Second Amendment exceed this Maximum Compensation without an approved change order. Continuant clearly understands and agrees, such understanding and agreement being of the absolute essence of this Agreement, that County shall have available the total maximum sum of $55,866.96, specifically allocated to fully discharge any and all liabilities County may incur. Continuant does further understand and agree, said understanding and agreement also being of the absolute essence of this Second Amendment, that the total maximum compensation that Continuant may become

entitled to and the total maximum sum that County may become liable to pay Continuant shall not under any conditions, circumstances, or interpretations thereof exceed $55,866.96. In no case shall the amount paid by County for all services under the Second Amendment exceed this Limit of Appropriation without an agreement executed by the parties.

D. **Human Trafficking**. BY ACCEPTANCE OF CONTRACT, CONTINUANT ACKNOWLEDGES THAT FORT BEND COUNTY IS OPPOSED TO HUMAN TRAFFICKING AND THAT NO COUNTY FUNDS WILL BE USED IN SUPPORT OF SERVICES OR ACTIVITIES THAT VIOLATE HUMAN TRAFFICKING LAWS.

E. **Modifications**. Except as modified herein, the Agreement remains in full force and effect and has not been modified or amended.

F. **Remote Access**. If Continuant requires remote access to County Systems for support, installation, integrations, configurations, and/or maintenance, except as otherwise agreed by the parties and approved by the County's Information Technology Director in writing, the below requirements must be met before Continuant is granted remote access to County Systems:

(1). Continuant will adhere to the restricted and monitored channels that are provided by the County, or other technologies approved in advanced in writing by the County's Information Technology Security Manager or the Assistant Information Technology Manager.

(2). Continuant will neither implement nor deploy a remote access solution which bypasses and/or is designed to bypass County provided or approved controls. Continuant will not access County Systems via unauthorized methods.

(3). Continuant's remote access to County Systems will only be requested and activated on as-needed basis and disabled when not in use.

(4). Remote access is restricted only to County Systems necessary for Continuant to conduct their services and/or provide product to County pursuant to this Second Amendment.

(5). Continuant will allow only its Workforce approved in advance by County to access County Systems. Continuant will promptly notify County whenever an individual member of Continuant's Workforce who has access to County Systems leaves its employ or no longer requires access to County Systems. Continuant will keep a log of access when its Workforce remotely accesses County Systems. Continuant will supply County with evidence of access logs concerning remote access to County Systems upon written request from County. Such access logs will be provided to County, within three business days from the date of County's request. These requests may be used to confirm compliance with these terms and/or to investigate a security incident.

(6). If any member(s) of Continuant's Workforce is provided with remote access to County Systems, then Continuant's workforce will not remotely log-in to

County Systems from a public internet access device (e.g., airport computer terminal, or Internet café). This is due to the possibility of sensitive information being monitored by video or computer surveillance in public areas.

(7). Failure of Continuant to comply with this Section may result in Continuant and/or Continuant's Workforce losing remote access to County Systems. County reserves the right at any time to disable remote access to protect County Systems.

(8). For purposes of this Section, "Workforce" means employees, agents, subcontractors (where permitted), and/or other persons whose conduct, in the performance of work for Continuant, is under the direct control of Continuant, whether or not they are paid by Continuant and who have direct or incidental access to County Systems.

(9). For purposes of this Section, "Systems" means any: (i.) computer programs, including, but not limited to, software, firmware, application programs, operating systems, files and utilities; (ii.) supporting documentation for such computer programs, including, without limitation, input and output formats, program listings, narrative descriptions and operating instructions; (iii.) data and/or media; (iv.) equipment, hardware, servers, and/or devices; and/or (v.) network(s).

G. **Conflict**. If there is a conflict among documents, the most recently executed document will prevail with regard to the conflict.

H. **Severability**. If any provision of the Agreement is determined to be invalid, illegal, or unenforceable, the remaining provisions remain in full force, if the essential terms and conditions of the Agreement for each party remain valid, binding, and enforceable.

(Execution Page Follows)

(Remainder of Page Intentionally Left Blank)

IN WITNESS WHEREOF, this Second Amendment is signed, accepted, and agreed to by all parties by and through the parties or their agents or authorized representatives. All parties hereby acknowledge that they have read and understood this Second Amendment and the attachments and exhibits hereto. All parties further acknowledge that they have executed this legal document voluntarily and of their own free will.

FORT BEND COUNTY	**CONTINUANT, INC.**
	DocuSigned by: Blair Duncan FE493C484A0A46F...
KP George County Judge	Authorized Agent – Signature
	Blair Duncan
Date	Authorized Agent- Printed Name
	CFO
ATTEST:	Title
	8-25-21
Laura Richard, County Clerk	Date

AUDITOR'S CERTIFICATE

I hereby certify that funds are available in the amount of_____ to accomplish and pay the obligation of Fort Bend County under this contract.

_____
Robert Edward Sturdivant, County Auditor

Exhibit 1: Addendum to Continuant, Inc.'s Agreement for Maintenance Advantage Plan Services FY 2021, executed by the parties on or about January 14, 2021, and as amended on or about June 22, 2021; and
Exhibit 2: Continuant's Statement of Work for the Maintenance Advantage Plan

Exhibit 1

STATE OF TEXAS §
§
COUNTY OF FORT BEND §

FIRST AMENDMENT TO ADDENDUM TO CONTINUANT, INC.'S AGREEMENT FOR MAINTENANCE ADVANTAGE PLAN SERVICES FY 2021

THIS FIRST AMENDMENT TO ADDENDUM TO CONTINUANT, INC.'S AGREEMENT FOR MAINTENANCE ADVANTAGE SERVICE PLAN SERVICES FY 2021 (the "First Amendment") is made and entered into by and between Fort Bend County, (hereinafter "County"), a body corporate and politic under the laws of the State of Texas, and Continuant, Inc., (hereinafter "Continuant"), a company authorized to conduct business in the State of Texas (collectively referred to as the "parties").

W I T N E S S E T H

WHEREAS, County and Continuant executed the Addendum to Continuant, Inc.'s Agreement for Maintenance Advantage Plan Services FY 2021 on or about January 14, 2021, (the "Agreement"), attached hereto as Exhibit I., and incorporated by reference, as if set forth herein verbatim. County and Continuant desire to amend the Agreement as set forth below:

A. **Scope of Services**. Continuant shall render additional services in accordance with Continuant's Statement of Work for the Maintenance Advantage Plan (Agreement Number: GSA #GS-35F-552AA), attached hereto as Exhibit II., and incorporated by reference.

B. **Term**. The term of this First Addendum is effective as of May 1, 2021, and shall expire no later than September 30, 2022, unless terminated sooner pursuant to the Agreement. Neither this First Amendment nor the Agreement shall automatically renew, but may be subsequently renewed in writing upon agreement of the parties.

C. **Limit of Appropriation**. Continuant's fees shall be calculated at the rates set forth in the attached Exhibit II. The Limit of Appropriation for the performance of services within the Scope of Services as described in Exhibit II. is $45,309.60. The Limit of Appropriation payable to Continuant for product and/or services rendered under the Agreement is hereby increased to an amount not to exceed $56,401.60, authorized as follows:

- $11,092.00 under the Agreement; and
- $45,309.60 under this First Amendment.

In no case shall the amount paid by County for all product and/or services under the Agreement and/or this First Amendment exceed the above Limit of Appropriation without an agreement executed by the parties. Additional funding

for this Agreement is contingent upon further appropriations from the County's Commissioners Court; the appropriation of additional funds is not guaranteed.

D. **Human Trafficking**. BY ACCEPTANCE OF CONTRACT, CONTINUANT ACKNOWLEDGES THAT FORT BEND COUNTY IS OPPOSED TO HUMAN TRAFFICKING AND THAT NO COUNTY FUNDS WILL BE USED IN SUPPORT OF SERVICES OR ACTIVITIES THAT VIOLATE HUMAN TRAFFICKING LAWS.

E. **Modifications**. Except as modified herein, the Agreement remains in full force and effect and has not been modified or amended.

F. **Conflict**. If there is a conflict among documents, the most recently executed document will prevail with regard to the conflict.

G. **Severability**. If any provision of the Agreement is determined to be invalid, illegal, or unenforceable, the remaining provisions remain in full force, if the essential terms and conditions of the Agreement for each party remain valid, binding, and enforceable.

(Execution Page Follows)

(Remainder of Page Intentionally Left Blank)

IN WITNESS WHEREOF, this First Amendment is signed, accepted, and agreed to by all parties by and through the parties or their agents or authorized representatives. All parties hereby acknowledge that they have read and understood this First Amendment and the attachments and exhibits hereto. All parties further acknowledge that they have executed this legal document voluntarily and of their own free will.

FORT BEND COUNTY

KP George
County Judge KP George
County Judge

6.22.2021
Date

ATTEST:

Laura Richard, County Clerk

CONTINUANT, INC.

DocuSigned by:
E831E292D7414A1...
Authorized Agent – Signature

Doug Graham
Authorized Agent- Printed Name

Title
Title

5/27/2021 | 8:07 AM PDT
Date

AUDITOR'S CERTIFICATE

I hereby certify that funds are available in the amount of $ 56,401.60 to accomplish and pay the obligation of Fort Bend County under this contract.

Robert Edward Sturdivant, County Auditor

Exhibit I: First Amendment to Addendum to Continuant, Inc.'s Agreement for Maintenance Advantage Plan Services, executed by the parties on or about January 14, 2021; and
Exhibit II: Continuant's Statement of Work for the Maintenance Advantage Plan

i:\agreements\2021 agreements\purchasing\it\continuant, inc. (21-it-100401)\continuant, inc. (21-it-100401-a1)\addendum to first amendment to agreement with continuant, inc..docx aw

Exhibit I.

STATE OF TEXAS §
§
COUNTY OF FORT BEND §

ADDENDUM TO CONTINUANT, INC.'S AGREEMENT FOR MAINTENANCE ADVANTAGE PLAN SERVICES FY 2021

THIS ADDENDUM ("Addendum") is entered into by and between Fort Bend County, ("County"), a body corporate and politic under the laws of the State of Texas, and Continuant, Inc., ("Continuant"), a company authorized to conduct business in the State of Texas (hereinafter collectively referred to as the "parties").

WHEREAS, the parties have executed and accepted Continuant's Statement of Work for the Maintenance Advantage Plan (Agreement Number: GSA #GS-35F-552AA), (the "Agreement"), attached hereto as Exhibit "A" and incorporated by reference, for the use of specified services and equipment (the "Services"); and

WHEREAS, the following changes are incorporated as if a part of the Agreement:

1. **Term**. The term of the Agreement is effective February 1, 2021, and shall expire no later than September 30, 2022, unless terminated sooner pursuant to the Agreement. This Agreement shall not automatically renew, but may be subsequently renewed in writing upon agreement of the parties.

2. **Payment; Non-appropriation; Taxes.** Payment shall be made by County within thirty (30) days of receipt of invoice. It is specifically understood and agreed that in the event no funds or insufficient funds are appropriated by Fort Bend County under this Agreement, Fort Bend County shall notify all necessary parties that this Agreement shall thereafter terminate and be null and void on the last day of the fiscal period for which appropriations were made without penalty, liability or expense to Fort Bend County. County is a body corporate and politic under the laws of the State of Texas and claims exemption from sales and use taxes. A copy of a tax-exempt certificate will be furnished upon request. Interest resulting from late payments by County shall be governed by Chapter 2251, TEXAS GOVERNMENT CODE.

3. **Limit of Appropriation.** Continuant clearly understands and agrees, such understanding and agreement being of the absolute essence of this Agreement, that County shall have available the total maximum sum of Eleven Thousand, Ninety-Two and 00/100 dollars ($11,092.00), specifically allocated to fully discharge any and all liabilities County may incur concerning this Agreement for County's Fiscal Year 2021. In no event will the amount paid by the County for all services under this Agreement exceed this Limit of Appropriation without an amendment executed by the parties. Additional funding for this Agreement for County's Fiscal Year 2022 is contingent upon further appropriations from the County's Commissioners Court; the appropriation of additional funds is not guaranteed.

4. **Public Information Act.** Continuant expressly acknowledges that County is subject to the Texas Public Information Act, TEX. GOV'T CODE ANN. §§ 552.001 *et seq.*, as amended, and notwithstanding any provision in the Agreement to the contrary, County will make any

information related to the Agreement, or otherwise, available to third parties in accordance with the Texas Public Information Act. Any proprietary or confidential information marked as such provided to County by Continuant shall not be disclosed to any third party, except as directed by the Texas Attorney General in response to a request for such under the Texas Public Information Act, which provides for notice to the owner of such marked information and the opportunity for the owner of such information to notify the Attorney General of the reasons why such information should not be disclosed. The terms and conditions of the Agreement are not proprietary or confidential information.

5. **Indemnity.** The parties agree that under the Constitution and laws of the State of Texas, County cannot enter into an agreement whereby County agrees to indemnify or hold harmless another party; therefore, all references of any kind to County defending, indemnifying, holding or saving harmless Continuant for any reason are hereby deleted. Continuant shall indemnify and defend County against all losses, liabilities, claims, causes of action, and other expenses, including reasonable attorney's fees, arising from activities of Continuant, its agents, servants or employees, performed under this agreement that result from the negligent act, error, or omission of Continuant or any of Continuant's agents, servants or employees.

6. **Applicable Law; Arbitration; Attorney Fees.** The laws of the State of Texas govern all disputes arising out of or relating to this Agreement. The parties hereto acknowledge that venue is proper in Fort Bend County, Texas, for all legal actions or proceedings arising out of or relating to this Agreement and waive the right to sue or be sued elsewhere. Nothing in the Agreement shall be construed to waive the County's sovereign immunity. County does not agree to submit disputes arising out of the Agreement to binding arbitration. Therefore, any references to binding arbitration or the waiver of a right to litigate a dispute are hereby deleted. County does not agree to pay any and/or all attorney fees incurred by Continuant in any way associated with the Agreement.

7. **Certain State Law Requirements for Contracts.** The contents of this Section are required by Texas Law and are included by County regardless of content.
   a. Agreement to Not Boycott Israel Chapter 2271 Texas Government Code: By signature below, Continuant verifies that if Continuant employs ten (10) or more full-time employees and this Agreement has a value of $100,000 or more, Continuant does not boycott Israel and will not boycott Israel during the term of this Agreement.
   b. Texas Government Code § 2252.152 Acknowledgment: By signature below, Continuant represents pursuant to § 2252.152 of the Texas Government Code, that Continuant is not listed on the website of the Comptroller of the State of Texas concerning the listing of companies that are identified under § 806.051, § 807.051, or § 2252.153.

8. **Modifications**. The parties may not amend or waive this Agreement, except by a written agreement executed by both Parties.

9. **Human Trafficking.** BY ACCEPTANCE OF CONTRACT, CONTINUANT ACKNOWLEDGES THAT FORT BEND COUNTY IS OPPOSED TO HUMAN

TRAFFICKING AND THAT NO COUNTY FUNDS WILL BE USED IN SUPPORT OF SERVICES OR ACTIVITIES THAT VIOLATE HUMAN TRAFFICKING LAWS.

10. **Use of Customer Name**. Continuant may use County's name without County's prior written consent only in any Continuant's customer lists, any other use must be approved in advance by County.

11. **Product Assurance.** Continuant represents and warrants that its hardware, software and any related systems and/or services related to its software and/or hardware (collectively, the "Product") furnished by Continuant to County will not infringe upon or violate any patent, copyright, trademark, trade secret, or any other proprietary right of any third party. Continuant will, at its expense, defend any suit brought against County and will indemnify County against an award of damages and costs (including reasonable attorney fees, court costs and appeals), made against County by settlement or final judgment of a court that is based on a claim that the use of Continuant's Product infringes an intellectual property right of a third party. Such defense and indemnity shall survive termination or expiration of the Agreement and Continuant's liability for the above is not limited by any limitation of liability clauses that may appear in any document executed by the Parties.

12. **Performance Warranty.** Continuant warrants to County that Continuant has the skill and knowledge ordinarily possessed by well-informed members of its trade or profession practicing in the greater Houston metropolitan area and Continuant will apply that skill and knowledge with care and diligence to ensure that the services provided hereunder will be performed and delivered in accordance with the highest professional standards.

13. **Conflict.** In the event there is a conflict between this Addendum and the Agreement, this Addendum controls.

14. **Understanding, Fair Construction.** By execution of this Addendum, the parties acknowledge that they have read and understood each provision, term and obligation contained in this Addendum. This Addendum, although drawn by one party, shall be construed fairly and reasonably and not more strictly against the drafting party than the nondrafting party.

15. **Captions**. The section captions used in this Agreement are for convenience of reference only and do not affect the interpretation or construction of this Agreement.

16. **Electronic and Digital Signatures.** The Parties to this Agreement agree that any electronic and/or digital signatures of the Parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as the use of manual signatures.

17. **Personnel**. Continuant represents that it presently has, or is able to obtain, adequate qualified personnel in its employment for the timely performance of the Services required under this Agreement and that Continuant shall furnish and maintain, at its own expense, adequate and sufficient personnel, in the opinion of County, to perform the Services when and as required and without delays.

All employees of Continuant shall have such knowledge and experience as will enable them to perform the duties assigned to them. Any employee of Continuant or agent of Continuant who, in the opinion of County, is incompetent or by his conduct becomes detrimental to providing Services pursuant to this Agreement shall, upon request of County, immediately be removed from association with the Services required under this Agreement.

Continuant will comply with any reasonable County security procedures concerning systems and data and remote access thereto, building security procedures, including the restriction of access by County to certain areas of its premises or systems for security reasons, and general health and safety practices and procedures or other written policies provided to Continuant as of the Effective Date, and thereafter as mutually agreed to by the parties.

18. **Compliance with Laws**. Continuant shall comply with all federal, state, and local laws, statutes, ordinances, rules and regulations, and the orders and decrees of any courts or administrative bodies or tribunals in any matter affecting the performance of this Agreement, including, without limitation, Worker's Compensation laws, minimum and maximum salary and wage statutes and regulations, licensing laws and regulations. When required by County, Continuant shall furnish County with certification of compliance with said laws, statutes, ordinances, rules, regulations, orders, and decrees above specified.

19. **Confidential Information.** Continuant acknowledges that it and its employees or agents may, in the course of performing their responsibilities under this Agreement, be exposed to or acquire information that is confidential to County. Any and all information of any form obtained by Continuant or its employees or agents from County in the performance of this Agreement shall be deemed to be confidential information of County ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Continuant shall be treated with respect to confidentiality in the same manner as the Confidential Information. Confidential Information shall be deemed not to include information that (a) is or becomes (other than by disclosure by Continuant) publicly known or is contained in a publicly available document; (b) is rightfully in Continuant's possession without the obligation of nondisclosure prior to the time of its disclosure under this Agreement; or (c) is independently developed by employees or agents of Continuant who can be shown to have had no access to the Confidential Information.

Continuant agrees to hold Confidential Information in strict confidence, using at least the same degree of care that Continuant uses in maintaining the confidentiality of its own confidential information, and not to copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than the provision of Services to County hereunder, and to advise each of its employees and agents of their obligations to keep Confidential Information confidential. Continuant shall use its best efforts to assist County in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limitation of the foregoing, Continuant shall advise County immediately in the event Continuant learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to

violate the terms of this Agreement and Continuant will at its expense cooperate with County in seeking injunctive or other equitable relief in the name of County or Continuant against any such person. Continuant agrees that, except as directed by County, Continuant will not at any time during or after the term of this Agreement disclose, directly or indirectly, any Confidential Information to any person, and that upon termination of this Agreement or at County's request, Continuant will promptly turn over to County all documents, papers, and other matter in Continuant's possession which embody Confidential Information.

Continuant acknowledges that a breach of this Section, including disclosure of any Confidential Information, or disclosure of other information that, at law or in equity, ought to remain confidential, will give rise to irreparable injury to County that is inadequately compensable in damages. Accordingly, County may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Continuant acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interest of County and are reasonable in scope and content.

Continuant in providing all services hereunder agrees to abide by the provisions of any applicable Federal or State Data Privacy Act.

20. **Termination.**

20.1. Termination for Convenience. County may terminate this Agreement at any time upon thirty (30) days written notice.

20.2. Termination for Default. County may terminate the whole or any part of this Agreement for cause in the following circumstances:

(a). If Continuant fails to timely perform services pursuant to this Agreement or any extension thereof granted by the County in writing;

(b). If Continuant materially breaches any of the covenants or terms and conditions set forth in this Agreement or fails to perform any of the other provisions of this Agreement or so fails to make progress as to endanger performance of this Agreement in accordance with its terms, and in any of these circumstances does not cure such breach or failure to County's reasonable satisfaction within a period of ten (10) calendar days after receipt of notice from County specifying such breach or failure.

20.3. If, after termination, it is determined for any reason whatsoever that Continuant was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the County in accordance with § 20.1 above.

20.4. Upon termination of this Agreement, County shall compensate Continuant in accordance with § 2, above, for those services which were provided under this Agreement prior to its termination and which have not been previously invoiced to County. Continuant's final invoice for said services will be presented to and paid by County in the same manner set forth in § 2 above.

20.5. If County terminates this Agreement as provided in this Section, no fees of any type, other than fees due and payable at the Termination Date, shall thereafter be paid to Continuant.

21. **Independent Contractor**. In the performance of work or services hereunder, Continuant shall be deemed an independent contractor, and any of its agents, employees, officers, or volunteers performing work required hereunder shall be deemed solely as employees of Continuant or, where permitted, of its subcontractors. Continuant and its agents, employees, officers, or volunteers shall not, by performing work pursuant to this Agreement, be deemed to be employees, agents, or servants of County and shall not be entitled to any of the privileges or benefits of County employment.

22. **Severability**. If any provision of this Agreement is determined to be invalid, illegal, or unenforceable, the remaining provisions remain in full force, if the essential terms and conditions of this Agreement for each party remain valid, binding, and enforceable.

23. **Insurance**. Prior to commencement of the Services under this Agreement, Continuant shall furnish County with properly executed certificates of insurance which shall evidence all insurance required and provide that such insurance shall not be canceled, except on 30 days' prior written notice to County. Continuant shall provide certified copies of insurance endorsements and/or policies if requested by County. Continuant shall maintain such insurance coverage from the time Services commence until Services are completed and provide replacement certificates, policies and/or endorsements for any such insurance expiring prior to completion of Services. Continuant shall obtain such insurance written on an Occurrence form from such companies having Bests rating of A/VII or better, licensed or approved to transact business in the State of Texas, and shall obtain such insurance of the following types and minimum limits:

(a). Workers' Compensation insurance. Substitutes to genuine Workers' Compensation Insurance will not be allowed. Employers' Liability insurance with limits of not less than $1,000,000 per injury by accident, $1,000,000 per injury by disease, and $1,000,000 per bodily injury by disease.

(b). Commercial general liability insurance with a limit of not less than $1,000,000 each occurrence and $2,000,000 in the annual aggregate. Policy shall cover liability for bodily injury, personal injury, and property damage and products/completed operations arising out of the business operations of the policyholder.

(c). Business Automobile Liability insurance with a combined Bodily Injury/Property Damage limit of not less than $1,000,000 each accident. The policy shall cover liability arising from the operation of licensed vehicles by policyholder.

(d). Professional Liability insurance with limits not less than $1,000,000.

County and the members of Commissioners Court shall be named as additional insured to all required coverage except for Workers' Compensation. All Liability policies including Workers' Compensation written on behalf of Continuant shall contain a waiver of subrogation in favor of County and members of Commissioners Court.

If required coverage is written on a claims-made basis, Continuant warrants that any retroactive date applicable to coverage under the policy precedes the effective date of the contract; and that continuous coverage will be maintained or an extended discovery period will be exercised for a period of two years beginning from the time that work under the Agreement is completed.

24. **Notices.**

24.1. Each party giving any notice or making any request, demand, or other communication (each, a "Notice") pursuant to this Agreement shall do so in writing and shall use one of the following methods of delivery, each of which, for purposes of this Agreement, is a writing: personal delivery, registered or certified mail (in each case, return receipt requested and postage prepaid), or nationally recognized overnight courier (with all fees prepaid).

24.2. Each party giving a Notice shall address the Notice to the receiving party at the address listed below or to another address designated by a party in a Notice pursuant to this Section:

County:	Fort Bend County Information Technology Attn: Information Technology Director 301 Jackson Street, Texas 77469
With a copy to:	Fort Bend County Attn: County Judge 401 Jackson Street Richmond, Texas 77469
Contractor:	Continuant, Inc. Attn:_____ 5050 20th Street East Fife, Washington 98424

24.3. A Notice is effective only if the party giving or making the Notice has complied with subsections 24.1 and 24.2 and if the addressee has received the Notice. A Notice is deemed received as follows:

24.3.1. If the Notice is delivered in person, or sent by registered or certified mail or a nationally recognized overnight courier, upon receipt as indicated by the date on the signed receipt.

24.3.2. If the addressee rejects or otherwise refuses to accept the Notice, or if the Notice cannot be delivered because of a change in address for which no Notice was given, then upon the rejection, refusal, or inability to deliver.

(Execution Page Follows)

(Remainder of Page Intentionally Left Blank)

IN WITNESS WHEREOF, this Addendum is signed, accepted, and agreed to by all parties by and through the parties or their agents or authorized representatives. All parties hereby acknowledge that they have read and understood this Addendum and the attachments and exhibits hereto. All parties further acknowledge that they have executed this legal document voluntarily and of their own free will.

FORT BEND COUNTY	**CONTINUANT, INC.**
Jaime Kovar	E831E292D7414A1...
Jaime Kovar	Authorized Agent – Signature
Purchasing Agent	Doug Graham
1/14/2021	
Date	Authorized Agent- Printed Name
REVIEWED:	CEO
	Title
Robyn Doughtie	1/7/2021 | 10:14 AM PST
Information Technology Department	Date

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of $ 11,092.00 are available to pay the obligation of Fort Bend County within the foregoing Agreement.

Robert Ed Sturdivant, County Auditor

Exhibit A: Continuant's Statement of Work for the Maintenance Advantage Plan (Agreement Number: GSA #GS-35F-552AA)

Exhibit A

Maintenance Advantage Plan

Continuant

Fort Bend County, TX ("CUSTOMER")

301 Jackson St.
Richmond, Texas 77469
(281) 342-3411
Agreement number: [GS-35F-552AA]

Continuant, Inc ("SUPPLIER")

5050 20th Street East
Fife, Washington 98424
(800) 652-9920

Statement of Work

Maintenance Advantage Plan

Base Plan Includes	
Event Management	
Incident Management	
Hardware Replacement	
Change Management	
Service Desk	
Service Level Management	
Optional Services	***Selected***
8/5 Onsite Incident Management	NO
24/7 Onsite Incident Management	YES
Simple Service Request	NO
Complex Service Request	NO
Projects	NO
Onsite Critical Spare Equipment	NO
Telephones & Attendant Console Coverage	NO
Carrier Services Management	NO
Set Up Fee	$ 600.00
Term: Coterminous to 09/30/2022	$ 1,049.20 /mo.
** Pricing valid until: 01/01/2021*	

Date of Commencement: 02/01/2021

Exhibit A

I agree to the terms and conditions of this Agreement.	Robyn Doughtie	1/13/2021
	Customer Signature	**Date**
	Robyn Doughtie	Fort Bend County IT Director
	Customer Print Signature	**Title**

Exhibit A

Description of Change

Adding 12 sites

Purpose

Scope of Work Purpose

The purpose of this Scope of Work is to document the scope of tasks Continuant shall undertake and responsibilities that Continuant shall assume as part of its obligation to provide Maintenance Support to the Customer and to document the allocation of responsibilities between the Parties with regard to certain operational processes.

Objectives

Objectives Overview

Continuant will provide Maintenance Support for the Customer's communications environment as agreed upon under this Scope of Work (SOW). The Customer desires to use these services to achieve certain business goals and objectives. The Parties have entered into this SOW to support achievement of the Customer's objectives. The Objectives are as follows:

- **Implement consistent services and processes governing the maintenance and management of the Customer's in-scope systems at the in-scope Sites on a global basis.**
- **Optimize and enhance the Customer's in-scope systems and realize continuous improvement in technology and service levels.**
- **Provided year-over-year reductions in the count and duration of outages through a high-touch service delivery experience, utilizing highly efficient processes and tools consistent with the IT Infrastructure Library (ITIL) and industry best practices.**

Services

Event Management

Continuant will provide 24x7 event management that includes system monitoring and management of events for both TDM and UC equipment where applicable. Continuant will identify critical components in customers' environment and define key events for the specific system components. Continuant will provide structured levels of notifications to the customer for significant events detected in the customers' environment. Continuant Event Management will trigger Incident Management where applicable.

Incident Management

Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized. Continuant is responsible for prioritization and management of all incidents throughout their lifecycles.

Remote Incident Management

Remote Incident Management is provided 24/7 and ensures that normal service operation is managed through remote connectivity. Remote incident management activities may include remote diagnostics, troubleshooting, and remote support for onsite personnel. Activities may include:

- Resolve service disruptions and performance degradations on Managed Components.
- Manage incident escalations to ensure timely and high-quality resolution of all issues by monitoring time remaining to meet SLAs.
- Utilize Incident remediation procedures to collect any additional data required to diagnose and match to known errors in Continuant knowledge base.
- Remote labor to repair or replace a failed part or device and the subsequent testing to confirm correct operation of the device and its interface and operation with associated equipment, communication facilities and services.
- Remotely facilitate hardware replacement and software updates determined to be required by Continuant.
- Utilize and update Continuant's ITSM platform with relevant information relating to an Incident.
- Make an initial determination of the potential resolution.
- Resolve as many Incidents as possible during the Authorized User's initial contact with the Service Desk, without transferring the call or using any escalation.
- Resolve Incidents requiring Tier 1-3 Support and close the Incident after receiving confirmation from the affected Authorized User that the Incident has been resolved.
- Resolve Incidents arising from or related to the Services, including break/fix Hardware and Software support.
- Retain overall responsibility and ownership of all Incidents until the Incident is closed subject to Customer approval.
- Software support services – includes remote installation assistance and basic usability assistance on minor firmware, patches and bug fixes (all managed components must include Original Equipment Manufacturer (OEM) software support coverage when applicable). Software support services do not include the purchase of subscriptions that provide entitlement and rights to use future minor versions (point

releases), future major releases of software, or patches.

Hardware Replacement

Continuant will provide hardware replacement on specified Covered Equipment. In the event of defective equipment, Continuant will make repairs or provide replacements of the defective equipment with either new equipment or a refurbished equivalent model at Continuant's discretion. Hardware Replacement includes parts within the telephone system (PBX) such as circuit packs, power supplies, processing elements and cabinetry, voicemail system (as applicable) and the primary server where a covered application resides. Telephone sets, power systems (UPS), PCs, servers, modems, routers, switches, wireless access points, security appliances, or other devices supporting carrier traffic are not included in this agreement unless specifically noted.

Change Management

Change Management is the process of assessing, controlling, managing and performing changes to a customer's infrastructure. The primary goal of this process is to ensure that changes are properly planned for, communicated, and approved. Change Management will consist of the following services:

- Continuant will follow the Request for Change (RFC) process. Providing the necessary documentation required to fulfill Change Requests. This will include associated plans required to implement the requested changes.

This process will be followed for Standard, Normal, and Emergency changes requested by the customer as agreed upon in this SOW. These changes are as follows:

- Standard – Standard changes are defined as well-known, repeatable and thoroughly documented procedures. These procedures present a low risk to operations and business services as determined by a standard risk assessment. Standard Changes are preauthorized by the Change Advisory Board to be implemented per terms agreed upon with the customer. If the Service owner is concerned about the risk and/or potential impact of a change on other services, then a Normal or Emergency change should be considered.

- Normal – Normal changes are defined as medium/high risk to business services and therefore must follow the normal change management process. Due to the potential risk and impact, normal changes must be reviewed, prioritized and scheduled by the Change Advisory Board (CAB). The Urgency of Normal Changes may be upgraded to accelerate the timeline for implementation given customer business justification of an impending business impact.

- Emergency – Emergency changes are defined as high risk to the business and required to be implemented as soon as possible – without proceeding through the normal change management process. They may be required to resolve a break/fix situation that has resulted in a service degradation or interruption in service. They may also be needed to address an imminent interruption in service. Emergency Changes should leverage existing Standard Change procedures where applicable to reduce the associated risk. These Changes should also be related to a corresponding Incident where a service disruption or potential disruption has been recorded.

Service Desk

The Continuant Global Service Desk will be the primary communication point for services. The Customer will have several ways of interacting with the Global Service Desk. Customer Service Desk activities shall include the following:

- Perform initial analysis, troubleshooting, and diagnostics for Event Management
- Fulfill Service Requests for the "Customer"
- Provide proactive communication of service delivery
- Manage escalations to ensure timely and high-quality resolution
- Provide life-cycle management of all service requests and incidents
- Provide Technical Support for general advice and help on covered systems

Network Operation Center Services

While most support organizations provide a one-time network assessment, Continuant provides an on-going assessment to consistently monitor, enhance, and improve the Customer's UC infrastructure.

- 24x7 event monitoring & management
- Perform initial analysis, troubleshooting, and diagnostics for Event Management

Technical Support

Continuant makes available to customers a dedicated team of engineers with OEM certifications to provide across-the-board Unified Communications Technical Support (TAC). TAC is designed to provide technical support for the customer when the customer has a

question about their covered environment. Customer can access Continuant TAC when following the below guidelines and attributes:

- Command Instructions
- Terminology Definitions
- Programming/Configurational Vetting
- Does not require changes or programming
- Does not require onsite technical resources
- Does not require scheduled maintenance window
- Does not require discovery
- Can be completed in 15 minutes or less.

Continuant TAC will stop at 15 minutes. All work will be billed at current Time and Material rates that exceed 15 minutes. Continuant will advise the customer of the rates and obtain customer approval before providing further support.

Service Level Management

Continuant's Service Level Management (SLM) offering tracks performance against negotiated service level targets called Service Level Agreements. SLM is also responsible for ensuring that all operational service level agreements and underpinning contracts are appropriate. Continuant will monitor and report on service levels where applicable and provide reports according to an agreed upon schedule. Service Level Agreements (SLAs) apply only to components that are managed exclusively by Continuant within the service. Continuant adheres to the SLAs during the Service Delivery phase. Within the Service Activation Kit (SAK), the Customer and Continuant must document their agreement to formally acknowledge the completion of the Service Transition process. The Service Delivery phase commences upon mutual agreement between Continuant and the Customer that the Service Transition phase is complete and that the Service Delivery phase has been reached.

The following metrics are tracked as Service Level Agreements:

- Time to Notify (TTN)
- Time to Restore (TTR)
- Time to Complete (TTC)

Incident Prioritization: Continuant classifies and prioritizes incidents according to Impact

and Urgency. Continuant will evaluate Incident Impact and Urgency to classify all Incidents into Priority 1 (P1), Priority 2 (P2), Priority 3 (P3) and Priority 4 (P4) Incident categories.

Continuant Incident Management Priorities Matrix

	Impact			
Urgency	Widespread	Large	Localized	Individualized
Critical	P1	P1	P2	P2
High	P1	P2	P2	P3
Medium	P2	P3	P3	P3
Low	P4	P4	P4	P4

Impact Definitions: An Incident is classified according to its impact on the business (the size, scope, and complexity of the Incident). Impact is a measure of the business criticality of an Incident, often equal to the extent to which an Incident leads to degradation of a Service. Continuant will work with Customer to specify Impact for each Managed Component during Service Transition. There are four Impact levels:

Widespread – Entire Network is affected (more than three quarters of individuals, sites or devices)

Large – Multiple sites are affected (between one-half and three-quarters of individuals, sites or devices)

Localized – Single site, room and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)

Individualized – A single user is affected (less than one-quarter of individuals, sites or devices)

Urgency Definition: Urgency defines the criticality of the Incident to Customer's business. Continuant will work with Customer to understand and set the proper Urgency level. There are four Urgency levels:

Critical – Primary business function is stopped with no redundancy or backup. There may be an immediate financial impact to Customer's business.

High – Primary business function is severely degraded or supported by backup or redundant system. There is potential for a significant financial impact to Customer's business.

Medium – Non-critical business function is stopped or severely degraded. There is a possible financial impact to Customer's business.

Low – Non-critical business function is degraded. There is little or no financial impact.

Time to Notify (TTN)

Customers may have specific notification requirements for which the Service will offer a Time to Notify (also known as "Respond") objective. Continuant will respond to incidents and requests raised through the management platform by electronically notifying a specified Customer contact(s) within the TTN timeframe. Continuant SLAs are as follows:

Case contact method	*Continuant estimated time to notify to specified contact*	*Incident or Service Request Level*	*SLA Target*
Event Managements Cases	15 Minutes from event opened date/time	All priority incidents	95%
Phone Call from "Customer"	15 Minutes from call being answered	All priority incidents and service requests	95%
Email from "Customer" to Service Desk	15 Minutes from email received date/time	All priority incidents and service requests	95%
Continuant MyCustomer Portal	15 Minutes from case opened date/time	All priority incidents and service requests	95%

Time to Restore (TTR)

Incidents go through many stages, with restoration being a primary objective. Time to Restore tickets includes all remote incident management activities (alarm or call receipt through restore, excluding maintenance or carrier cycle time). TTR refers to the time elapsed between the failure which caused the incident and when Continuant restores the managed component to an acceptable operational state. Continuant SLAs for meeting this objective are as follows:

Incident Level	*Time to Restore*	*SLA Target*

Exhibit A

P1 Incidents	4 Hours	95%
P2 Incidents	12 Hours	95%
P3 Incidents	72 Hours	95%
P4 Incidents	120 Hours	95%

SLA measurements exclude the following:

- Delays caused by Customer in resolving the qualifying issue (for example, waiting for response on change window or on-site resources).
- Any mutually agreed upon schedule of activities that causes service levels to fall outside of measured SLAs defined obligations.
- SLAs will be paused for hardware replacement delivery to the customer location, either from a manufacturer maintenance agreement or hardware replacement services from Continuant.
- Delays or faults caused by third party equipment, services or vendors, such as Carriers, in resolving the qualifying issue.
- Other factors outside of Continuant's reasonable control for which Continuant is not responsible.
- Acquisition and installation time of new software to be installed on the Managed Component due to software defects or bugs.

Time to Complete (TTC)

Continuant has categorized requests based on level of risk, complexity and the amount of time required to complete the request. All Changes are scheduled events and are dependent on coordination with Customer's schedule. A change request must be fully qualified and scheduled with Customer before the Time to Complete metric starts. All custom requests for change are scheduled events and follow the Normal Change Management procedures.

The chart below provides a breakdown of the available categories and durations for three types of requests.

Continuant SLAs for completing requests are as follows:

Change Request	Time to completion from receipt of fully qualified and scheduled change request	SLA Target
Remote Simple	2 business days	95%
Remote Simple – Expedited	8 hours	95%
Complex	Within 5 business days*	95%
Project	No SLA, scheduled	No SLA

**SLA time commences upon Continuant receiving signed quote from Customer.*

**Enhanced entitlements are available at a premium.*

SLA measurements exclude the following:

- Delays caused by Customer in executing the requested change (for example, waiting for response on change window).
- Any mutually agreed upon schedule of activities that causes service levels to fall outside of measured SLAs defined obligations.
- Other factors outside of Continuant's reasonable control for which Continuant is not responsible.
- Ticket closure time may be different than change completion time. For example: a ticket may be kept open for review after the change has been executed.

Any Customer-requested changes that are considered by the Customer as "emergency" or "urgent" changes will be treated on a commercially reasonable effort by the Continuant Service Desk and will depend on Continuant engineer availability at the time of submittal. Additional charges may apply.

Additional Managed Services

*Only applies to Optional MAP Services listed on page 1 of this Scope of Work with YES in the "Selected" column.

24/7 Onsite Incident Management

Continuant will provide 24/7 Onsite Support that ensures normal service operation is restored as quickly as possible and the business impact is minimized through dispatch of local technicians. Continuant is responsible for managing the lifecycle of all incidents. Activities may include 24/7 Dispatch of local technicians for diagnostics, troubleshooting and/or parts replacement (parts not included unless they are covered under Hardware Replacement Services). Customer ensures 24/7 access.

Other Information

Continuant Remote Access and Monitoring Platform

The Continuant-owned Secure Access Server (SAS) will allow remote access and monitoring for all managed systems supported by Continuant. The SAS contains all management software and hardware required for the delivery of services. The SAS is securely deployed on the Customer's network in a single configuration instance or multiple instance configurations depending on the number, type, and location of the managed components. During the coverage term, Customers are granted a nonexclusive and nontransferable license to use the hardware and the software resident solely on the SAS supplied by Continuant. Customers must return any and all associated SAS materials and connectivity devices to Continuant immediately upon expiration or termination of the agreement. Any delay by the Customer with supporting these Remote Access requirements may result in time and material charges for maintenance services. The Continuant SAS security compliance documentation is available upon request.

Asset Management

Continuant's Asset Management standard service will use the Service Activation Kit (SAK) information listed in the Customer Responsibilities section below to capture specific information for the Covered Equipment that includes the following:

- Serial Number
- Model Number
- System Firmware\Operating version
- Physical Location to include;
  - Street Address,
  - Floor Number
  - Room Number
  - Rack Location (if Applicable)
  - Brief description of the location
- Credentials for accessing and resolving issues with the equipment (May require top level admin/root)

Customer Responsibilities

The Customer is responsible for completing a Service Activation Kit (SAK), which provides Continuant the key information critical to success for commencement of maintenance. The

Customer will complete tasks defined in the SAK to enable management access to Covered Equipment which may include setting up SNMP traps, and system logs. These activities are both critical and beneficial to the Customer and Continuant as these activities establish a managed connection required for Continuant to resolve incidents and service requests quickly.
Items in the SAK include:

- Customer representative contact name
- Location of the site(s) to be managed
- Location of management applications
- Network connectivity approval and placement detail for the SAS
- Device location and naming scheme
- Management IP addresses and system detail, SNMP community strings
- Access method and credentials (Telnet, Remote Desktop, etc.)
- Management system User names and contact detail
- Installation of the SAS and network connectivity per Continuant-supplied guidelines.
- Communications facilities and services including internet and network configuration. The communication facilities and services must be maintained for the duration of the service term.
- Resource to support the installation activities of the SAS, which may include:
  - Racking
  - Connection to Network
  - Power connection to UPS or other facility with continuous uninterrupted power
  - Provide suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the SAS.

**Any delay or error by the customer in providing this information could delay commencement date.*

Location & Covered Equipment

Location Name	Services & Equipment	Paid Monthly	Paid Annually
Cinco Ranch • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) 24/7 Onsite Incident Management-NV G430 Gateway • G430 MP120 MEDIA GATEWAY – 1 unit(s)	$ 50.00	$ 600.00
First Colony • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) 24/7 Onsite Incident Management-NV G430 Gateway • G430 MP120 MEDIA GATEWAY – 1 unit(s)	$ 50.00	$ 600.00
Fulshear • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER - NON GSA – 1 unit(s) 24/7 Onsite Incident Management-NV G430 Gateway • G430 MP120 MEDIA GATEWAY – 1 unit(s)	$ 50.00	$ 600.00
GM-Admin • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) G450 Gateway • G450 MP80 W/POWER SUPPLY NON-GSA – 1 unit(s) 24/7 Onsite Incident Management-NV	$ 50.00	$ 600.00
Library Main • DOC: 02/01/2021	Avaya VM Base Plan • Avaya CM Messaging – 60 user(s) Large Server Support (CSS) • Session Manager – 1 server(s) • DL360PG8 SERVER AURA MESSAGING STANDARD STORAGE – 1 server(s) 24/7 Onsite Incident Management • Avaya CM Messaging – 60 user(s) • Avaya CM v7 – 60 user(s) • Session Manager – 1 server(s) • DL360PG8 SERVER AURA MESSAGING STANDARD STORAGE – 1 server(s) • Avaya G650 Media Gateway RHS Phone System – 4 unit(s) Avaya PBX Base Plan	$ 499.20	$ 5,990.40

Exhibit A

Location Name	Services & Equipment	Paid Monthly	Paid Annually
	• Avaya CM v7 – 60 user(s) G650 Gateway • Avaya G650 Media Gateway RHS Phone System – 4 unit(s)		
Mission Bend • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER - NON GSA VIRTUALIZATION PLATFORM – 1 unit(s) 24/7 Onsite Incident Management-NV G430 Gateway • G430 MP120 MEDIA GATEWAY NON GSA – 1 unit(s)	$ 50.00	$ 600.00
Missouri City • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) G450 Gateway • G450 CHASSIS/MAIN BOARD/80 CHANNEL DSP DAUGHTERBOARD/1 PSU – 1 unit(s) 24/7 Onsite Incident Management-NV	$ 50.00	$ 600.00
Needville • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER - NON GSA – 1 unit(s) 24/7 Onsite Incident Management-NV G430 Gateway • G430 MP120 MEDIA GATEWAY – 1 unit(s)	$ 50.00	$ 600.00
Sienna • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) G450 Gateway • G450 CHASSIS/MAIN BOARD/20 CHANNEL DSP DAUGHTERBOARD/1 PSU – 1 unit(s) 24/7 Onsite Incident Management-NV	$ 50.00	$ 600.00
Stafford • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) 24/7 Onsite Incident Management-NV G430 Gateway • G430 MP120 MEDIA GATEWAY – 1 unit(s)	$ 50.00	$ 600.00
Sugar Land • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER - NON GSA – 1 unit(s) G450 Gateway	$ 50.00	$ 600.00

Location Name	Services & Equipment	Paid Monthly	Paid Annually
	• G450 CHASSIS/MAIN BOARD/80 CHANNEL DSP DAUGHTERBOARD/1 PSU – 1 unit(s) 24/7 Onsite Incident Management-NV		
University • DOC: 02/01/2021	Additional Equipment - Base Plan • S8300E SERVER – 1 unit(s) G450 Gateway • G450 MP80 W/POWER SUPPLY NON-GSA – 1 unit(s) 24/7 Onsite Incident Management-NV	$ 50.00	$ 600.00

Exhibit II.

Maintenance Advantage Plan

Continuant

Fort Bend County, TX ("CUSTOMER")

301 Jackson St.
Richmond , Texas 77469
(281) 342-3411
Agreement number: [GS-35F-552AA]

Continuant, Inc ("SUPPLIER")

5050 20th Street East
Fife , Washington 98424
(800) 652-9920

Statement of Work

Maintenance Advantage Plan

Base Plan Includes	
Event Management	
Incident Management	
Hardware Replacement	
Change Management	
Service Desk	
Service Level Management	
Optional Services	***Selected***
8/5 Onsite Incident Management	**NO**
24/7 Onsite Incident Management	**YES**
Simple Service Request	**NO**
Complex Service Request	**NO**
Projects	**NO**
Onsite Critical Spare Equipment	**NO**
Telephones & Attendant Console Coverage	**NO**
Carrier Services Management	**NO**
Term: Coterminous to 09/30/2022	**$ 3,775.80 /mo.**
** Pricing valid until: 04/19/2021*	

Date of Commencement: 04/01/2021

I agree to the terms and conditions of this Agreement.

Customer Signature	Date
Customer Print Signature	Title

Purpose

Scope of Work Purpose

The purpose of this Scope of Work is to document the scope of tasks Continuant shall undertake and responsibilities that Continuant shall assume as part of its obligation to provide Maintenance Support to the Customer and to document the allocation of responsibilities between the Parties with regard to certain operational processes.

Objectives

Objectives Overview

Continuant will provide Maintenance Support for the Customer's communications environment as agreed upon under this Scope of Work (SOW). The Customer desires to use these services to achieve certain business goals and objectives. The Parties have entered into this SOW to support achievement of the Customer's objectives. The Objectives are as follows:

- Implement consistent services and processes governing the maintenance and management of the Customer's in-scope systems at the in-scope Sites on a global basis.
- Optimize and enhance the Customer's in-scope systems and realize continuous improvement in technology and service levels.
- Provided year-over-year reductions in the count and duration of outages through a high-touch service delivery experience, utilizing highly efficient processes and tools consistent with the IT Infrastructure Library (ITIL) and industry best practices.

Services

Event Management

Continuant will provide 24x7 event management that includes system monitoring and management of events for both TDM and UC equipment where applicable. Continuant will identify critical components in customers' environment and define key events for the specific system components. Continuant will provide structured levels of notifications to the customer for significant events detected in the customers' environment. Continuant Event Management will trigger Incident Management where applicable.

Incident Management

Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized. Continuant is responsible for prioritization and management of all incidents throughout their lifecycles.

Remote Incident Management

Remote Incident Management is provided 24/7 and ensures that normal service operation is managed through remote connectivity. Remote incident management activities may include remote diagnostics, troubleshooting, and remote support for onsite personnel. Activities may include:

- Resolve service disruptions and performance degradations on Managed Components.
- Manage incident escalations to ensure timely and high-quality resolution of all issues by monitoring time remaining to meet SLAs.
- Utilize Incident remediation procedures to collect any additional data required to diagnose and match to known errors in Continuant knowledge base.
- Remote labor to repair or replace a failed part or device and the subsequent testing to confirm correct operation of the device and its interface and operation with associated equipment, communication facilities and services.
- Remotely facilitate hardware replacement and software updates determined to be required by Continuant.
- Utilize and update Continuant's ITSM platform with relevant information relating to an Incident.
- Make an initial determination of the potential resolution.
- Resolve as many Incidents as possible during the Authorized User's initial contact with the Service Desk, without transferring the call or using any escalation.
- Resolve Incidents requiring Tier 1-3 Support and close the Incident after receiving confirmation from the affected Authorized User that the Incident has been resolved.
- Resolve Incidents arising from or related to the Services, including break/fix Hardware and Software support.
- Retain overall responsibility and ownership of all Incidents until the Incident is closed subject to Customer approval.
- Software support services – includes remote installation assistance and basic usability assistance on minor firmware, patches and bug fixes (all managed components must include Original Equipment Manufacturer (OEM) software support coverage when applicable). Software support services do not include the purchase of subscriptions that provide entitlement and rights to use future minor versions (point releases), future major releases of software, or patches.

Hardware Replacement

Continuant will provide hardware replacement on specified Covered Equipment. In the event of defective equipment, Continuant will make repairs or provide replacements of the defective equipment with either new equipment or a refurbished equivalent model at Continuant's discretion. Hardware Replacement includes parts within the telephone system (PBX) such as circuit packs, power supplies, processing elements and cabinetry, voicemail system (as applicable) and the primary server where a covered application resides. Telephone sets, power systems (UPS), PCs, servers, modems, routers, switches, wireless access points, security appliances, or other devices supporting carrier traffic are not included in this agreement unless specifically noted.

Change Management

Change Management is the process of assessing, controlling, managing and performing changes to a customer's infrastructure. The primary goal of this process is to ensure that changes are properly planned for, communicated, and approved. Change Management will consist of the following services:

- Continuant will follow the Request for Change (RFC) process. Providing the necessary documentation required to fulfill Change Requests. This will include associated plans required to implement the requested changes.

This process will be followed for Standard, Normal, and Emergency changes requested by the customer as agreed upon in this SOW. These changes are as follows:

- Standard – Standard changes are defined as well-known, repeatable and thoroughly documented procedures. These procedures present a low risk to operations and business services as determined by a standard risk assessment. Standard Changes are preauthorized by the Change Advisory Board to be implemented per terms agreed upon with the customer. If the Service owner is concerned about the risk and/or potential impact of a change on other services, then a Normal or Emergency change should be considered.

- Normal – Normal changes are defined as medium/high risk to business services and therefore must follow the normal change management process. Due to the potential risk and impact, normal changes must be reviewed, prioritized and scheduled by the Change Advisory Board (CAB). The Urgency of Normal Changes may be upgraded to accelerate the timeline for implementation given customer business justification of an impending business impact.

- Emergency – Emergency changes are defined as high risk to the business and required to be implemented as soon as possible – without proceeding through the normal change management process. They may be required to resolve a break/fix situation that has resulted in a service degradation or interruption in service. They may also be needed to

address an imminent interruption in service. Emergency Changes should leverage existing Standard Change procedures where applicable to reduce the associated risk. These Changes should also be related to a corresponding Incident where a service disruption or potential disruption has been recorded.

Service Desk

The Continuant Global Service Desk will be the primary communication point for services. The Customer will have several ways of interacting with the Global Service Desk. Customer Service Desk activities shall include the following:

- Perform initial analysis, troubleshooting, and diagnostics for Event Management
- Fulfill Service Requests for the “Customer”
- Provide proactive communication of service delivery
- Manage escalations to ensure timely and high-quality resolution
- Provide life-cycle management of all service requests and incidents
- Provide Technical Support for general advice and help on covered systems

Network Operation Center Services

While most support organizations provide a one-time network assessment, Continuant provides an on-going assessment to consistently monitor, enhance, and improve the Customer’s UC infrastructure.

- 24x7 event monitoring & management
- Perform initial analysis, troubleshooting, and diagnostics for Event Management

Technical Support

Continuant makes available to customers a dedicated team of engineers with OEM certifications to provide across-the-board Unified Communications Technical Support (TAC). TAC is designed to provide technical support for the customer when the customer has a question about their covered environment. Customer can access Continuant TAC when following the below guidelines and attributes:

- Command Instructions
- Terminology Definitions

- Programming/Configurational Vetting
- Does not require changes or programming
- Does not require onsite technical resources
- Does not require scheduled maintenance window
- Does not require discovery
- Can be completed in 15 minutes or less.

Continuant TAC will stop at 15 minutes. All work will be billed at current Time and Material rates that exceed 15 minutes. Continuant will advise the customer of the rates and obtain customer approval before providing further support.

Service Level Management

Continuant's Service Level Management (SLM) offering tracks performance against negotiated service level targets called Service Level Agreements. SLM is also responsible for ensuring that all operational service level agreements and underpinning contracts are appropriate. Continuant will monitor and report on service levels where applicable and provide reports according to an agreed upon schedule. Service Level Agreements (SLAs) apply only to components that are managed exclusively by Continuant within the service. Continuant adheres to the SLAs during the Service Delivery phase. Within the Service Activation Kit (SAK), the Customer and Continuant must document their agreement to formally acknowledge the completion of the Service Transition process. The Service Delivery phase commences upon mutual agreement between Continuant and the Customer that the Service Transition phase is complete and that the Service Delivery phase has been reached.

The following metrics are tracked as Service Level Agreements:

- Time to Notify (TTN)
- Time to Restore (TTR)
- Time to Complete (TTC)

Incident Prioritization: Continuant classifies and prioritizes incidents according to Impact and Urgency. Continuant will evaluate Incident Impact and Urgency to classify all Incidents into Priority 1 (P1), Priority 2 (P2), Priority 3 (P3) and Priority 4 (P4) Incident categories.

Continuant Incident Management Priorities Matrix

	Impact			
Urgency	Widespread	Large	Localized	Individualized
Critical	P1	P1	P2	P2
High	P1	P2	P2	P3
Medium	P2	P3	P3	P3
Low	P4	P4	P4	P4

Impact Definitions: An Incident is classified according to its impact on the business (the size, scope, and complexity of the Incident). Impact is a measure of the business criticality of an Incident, often equal to the extent to which an Incident leads to degradation of a Service. Continuant will work with Customer to specify Impact for each Managed Component during Service Transition. There are four Impact levels:

Widespread – Entire Network is affected (more than three quarters of individuals, sites or devices)

Large – Multiple sites are affected (between one-half and three-quarters of individuals, sites or devices)

Localized – Single site, room and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)

Individualized – A single user is affected (less than one-quarter of individuals, sites or devices)

Urgency Definition: Urgency defines the criticality of the Incident to Customer's business. Continuant will work with Customer to understand and set the proper Urgency level. There are four Urgency levels:

Critical – Primary business function is stopped with no redundancy or backup. There may be an immediate financial impact to Customer's business.

High – Primary business function is severely degraded or supported by backup or redundant system. There is potential for a significant financial impact to Customer's business.

Medium – Non-critical business function is stopped or severely degraded. There is a possible financial impact to Customer's business.

Low – Non-critical business function is degraded. There is little or no financial impact.

Time to Notify (TTN)

Customers may have specific notification requirements for which the Service will offer a Time to Notify (also known as "Respond") objective. Continuant will respond to incidents and requests raised through the management platform by electronically notifying a specified Customer contact(s) within the TTN timeframe. Continuant SLAs are as follows:

Case contact method	*Continuant estimated time to notify to specified contact*	*Incident or Service Request Level*	*SLA Target*
Event Managements Cases	15 Minutes from event opened date/time	All priority incidents	95%
Phone Call from "Customer"	15 Minutes from call being answered	All priority incidents and service requests	95%
Email from "Customer" to Service Desk	15 Minutes from email received date/time	All priority incidents and service requests	95%
Continuant MyCustomer Portal	15 Minutes from case opened date/time	All priority incidents and service requests	95%

Time to Restore (TTR)

Incidents go through many stages, with restoration being a primary objective. Time to Restore tickets includes all remote incident management activities (alarm or call receipt through restore, excluding maintenance or carrier cycle time). TTR refers to the time elapsed between the failure which caused the incident and when Continuant restores the managed component to an acceptable operational state. Continuant SLAs for meeting this objective are as follows:

Incident Level	*Time to Restore*	*SLA Target*
P1 Incidents	4 Hours	95%
P2 Incidents	12 Hours	95%

P3 Incidents	72 Hours	95%
P4 Incidents	120 Hours	95%

SLA measurements exclude the following:

- Delays caused by Customer in resolving the qualifying issue (for example, waiting for response on change window or on-site resources).
- Any mutually agreed upon schedule of activities that causes service levels to fall outside of measured SLAs defined obligations.
- SLAs will be paused for hardware replacement delivery to the customer location, either from a manufacturer maintenance agreement or hardware replacement services from Continuant.
- Delays or faults caused by third party equipment, services or vendors, such as Carriers, in resolving the qualifying issue.
- Other factors outside of Continuant's reasonable control for which Continuant is not responsible.
- Acquisition and installation time of new software to be installed on the Managed Component due to software defects or bugs.

Time to Complete (TTC)

Continuant has categorized requests based on level of risk, complexity and the amount of time required to complete the request. All Changes are scheduled events and are dependent on coordination with Customer's schedule. A change request must be fully qualified and scheduled with Customer before the Time to Complete metric starts. All custom requests for change are scheduled events and follow the Normal Change Management procedures.

The chart below provides a breakdown of the available categories and durations for three types of requests.

Continuant SLAs for completing requests are as follows:

Change Request	*Time to completion from receipt of fully qualified and scheduled change request*	*SLA Target*
Remote Simple	2 business days	95%
Remote Simple – Expedited	8 hours	95%
Complex	Within 5 business days*	95%
Project	No SLA, scheduled	No SLA

**SLA time commences upon Continuant receiving signed quote from Customer.*

**Enhanced entitlements are available at a premium.*

SLA measurements exclude the following:

- Delays caused by Customer in executing the requested change (for example, waiting for response on change window).
- Any mutually agreed upon schedule of activities that causes service levels to fall outside of measured SLAs defined obligations.
- Other factors outside of Continuant's reasonable control for which Continuant is not responsible.
- Ticket closure time may be different than change completion time. For example: a ticket may be kept open for review after the change has been executed.

Any Customer-requested changes that are considered by the Customer as "emergency" or "urgent" changes will be treated on a commercially reasonable effort by the Continuant Service Desk and will depend on Continuant engineer availability at the time of submittal. Additional charges may apply.

Additional Managed Services

*Only applies to Optional MAP Services listed on page 1 of this Scope of Work with YES in the "Selected" column.

24/7 Onsite Incident Management

Continuant will provide 24/7 Onsite Support that ensures normal service operation is restored as quickly as possible and the business impact is minimized through dispatch of local

technicians. Continuant is responsible for managing the lifecycle of all incidents. Activities may include 24/7 Dispatch of local technicians for diagnostics, troubleshooting and/or parts replacement (parts not included unless they are covered under Hardware Replacement Services). Customer ensures 24/7 access.

Other Information

Continuant Remote Access and Monitoring Platform

The Continuant-owned Secure Access Server (SAS) will allow remote access and monitoring for all managed systems supported by Continuant. The SAS contains all management software and hardware required for the delivery of services. The SAS is securely deployed on the Customer's network in a single configuration instance or multiple instance configurations depending on the number, type, and location of the managed components. During the coverage term, Customers are granted a nonexclusive and nontransferable license to use the hardware and the software resident solely on the SAS supplied by Continuant. Customers must return any and all associated SAS materials and connectivity devices to Continuant immediately upon expiration or termination of the agreement. Any delay by the Customer with supporting these Remote Access requirements may result in time and material charges for maintenance services. The Continuant SAS security compliance documentation is available upon request.

Asset Management

Continuant's Asset Management standard service will use the Service Activation Kit (SAK) information listed in the Customer Responsibilities section below to capture specific information for the Covered Equipment that includes the following:

- Serial Number
- Model Number
- System Firmware\Operating version
- Physical Location to include;
  - Street Address,
  - Floor Number
  - Room Number
  - Rack Location (if Applicable)
  - Brief description of the location
- Credentials for accessing and resolving issues with the equipment (May require top level admin/root)

Customer Responsibilities

The Customer is responsible for completing a Service Activation Kit (SAK), which provides Continuant the key information critical to success for commencement of maintenance. The Customer will complete tasks defined in the SAK to enable management access to Covered Equipment which may include setting up SNMP traps, and system logs. These activities are both critical and beneficial to the Customer and Continuant as these activities establish a managed

connection required for Continuant to resolve incidents and service requests quickly.
Items in the SAK include:

- Customer representative contact name
- Location of the site(s) to be managed
- Location of management applications
- Network connectivity approval and placement detail for the SAS
- Device location and naming scheme
- Management IP addresses and system detail, SNMP community strings
- Access method and credentials (Telnet, Remote Desktop, etc.)
- Management system User names and contact detail
- Installation of the SAS and network connectivity per Continuant-supplied guidelines.
- Communications facilities and services including internet and network configuration. The communication facilities and services must be maintained for the duration of the service term.
- Resource to support the installation activities of the SAS, which may include:
  - Racking
  - Connection to Network
  - Power connection to UPS or other facility with continuous uninterrupted power
  - Provide suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the SAS.

**Any delay or error by the customer in providing this information could delay commencement date.*

Location & Covered Equipment

Location Name	*Services & Equipment*	*Paid Monthly*	*Paid Annually*
Sheriff's Office • DOC: 04/01/2021	Avaya PBX Base Plan • Avaya CM – 850 user(s) G650 Gateway • G650 – 3 unit(s) 24/7 Onsite Incident Management • G650 – 3 qty. • Session Manager – 1 server(s) • Avaya CM – 850 user(s) • Avaya CM Messaging – 850 user(s) Avaya VM Base Plan • Avaya CM Messaging – 850 user(s) Large Server Support (CSS) • Session Manager – 1 server(s)	$ 3,775.80	$ 45,309.60

CERTIFICATE OF INTERESTED PARTIES

FORM 1295

Complete Nos. 1 - 4 and 6 if there are interested parties.
Complete Nos. 1, 2, 3, 5, and 6 if there are no interested parties.

OFFICE USE ONLY
CERTIFICATION OF FILING

Certificate Number:
2021-760335

Date Filed:
06/01/2021

Date Acknowledged:

1 Name of business entity filing form, and the city, state and country of the business entity's place of business.

Continuant, Inc.
FifeFife, WA United States

2 Name of governmental entity or state agency that is a party to the contract for which the form is being filed.

Fort Bend County

3 Provide the identification number used by the governmental entity or state agency to track or identify the contract, and provide a description of the services, goods, or other property to be provided under the contract.

28089
25/7 Onsite incident management

4 Name of Interested Party	City, State, Country (place of business)	Nature of interest (check applicable)	
		Controlling	Intermediary

5 Check only if there is NO Interested Party. [X]

6 UNSWORN DECLARATION

My name is Samuel Mosier, and my date of birth is 9/7/1975.

My address is 5050 20th St. E. (street), Fife (city), WA (state), 98424 (zip code), USA (country).

I declare under penalty of perjury that the foregoing is true and correct.

Executed in Pierce County, State of Washington, on the 1 day of June (month), 2021 (year).

Signature of authorized agent of contracting business entity
(Declarant)

CERTIFICATE OF INTERESTED PARTIES

FORM 1295

Complete Nos. 1 - 4 and 6 if there are interested parties.
Complete Nos. 1, 2, 3, 5, and 6 if there are no interested parties.

OFFICE USE ONLY
CERTIFICATION OF FILING

Certificate Number:
2021-760335

Date Filed:
06/01/2021

Date Acknowledged:
06/23/2021

1 Name of business entity filing form, and the city, state and country of the business entity's place of business.

Continuant, Inc.
FifeFife, WA United States

2 Name of governmental entity or state agency that is a party to the contract for which the form is being filed.

Fort Bend County

3 Provide the identification number used by the governmental entity or state agency to track or identify the contract, and provide a description of the services, goods, or other property to be provided under the contract.

28089
25/7 Onsite incident management

4 Name of Interested Party	City, State, Country (place of business)	Nature of interest (check applicable)	
		Controlling	Intermediary

5 Check only if there is NO Interested Party. [X]

6 UNSWORN DECLARATION

My name is _____, and my date of birth is _____.

My address is _____, _____, _____, _____, _____.
(street) (city) (state) (zip code) (country)

I declare under penalty of perjury that the foregoing is true and correct.

Executed in _____County, State of _____, on the _____day of _____, 20_____.
(month) (year)

_____
Signature of authorized agent of contracting business entity
(Declarant)

Exhibit 2

Maintenance Advantage Plan

Continuant

Fort Bend County, TX ("CUSTOMER")

301 Jackson St.
Richmond , Texas 77469
(281) 342-3411
Agreement number: [GSA #GS-35F-552AA]

Continuant, Inc ("SUPPLIER")

5050 20th Street East
Fife , Washington 98424
(800) 652-9920

Statement of Work

Maintenance Advantage Plan

Base Plan Includes	
Event Management	
Incident Management	
Hardware Replacement	
Change Management	
Service Desk	
Service Level Management	
Optional Services	***Selected***
8/5 Onsite Incident Management	**NO**
24/7 Onsite Incident Management	**YES**
Simple Service Request	**NO**
Complex Service Request	**NO**
Projects	**NO**
Onsite Critical Spare Equipment	**NO**
Telephones & Attendant Console Coverage	**NO**
3rd Party Vendor Management	**NO**
Term: 12 Months*	**$ 4,655.58 /mo.**
** Pricing valid until: 10/31/2021*	

Date of Commencement: 10/01/2021

Exhibit 2

I agree to the terms and conditions of this Agreement.

Customer Signature	Date
Customer Print Signature	Title

Purpose

Scope of Work Purpose

The purpose of this Scope of Work is to document the scope of tasks Continuant shall undertake and responsibilities that Continuant shall assume as part of its obligation to provide Maintenance Support to the Customer and to document the allocation of responsibilities between the Parties with regard to certain operational processes.

Objectives

Objectives Overview

Continuant will provide Maintenance Support for the Customer's communications environment as agreed upon under this Scope of Work (SOW). The Customer desires to use these services to achieve certain business goals and objectives. The Parties have entered into this SOW to support achievement of the Customer's objectives. The Objectives are as follows:

- Implement consistent services and processes governing the maintenance and management of the Customer's in-scope systems at the in-scope Sites on a global basis.
- Optimize and enhance the Customer's in-scope systems and realize continuous improvement in technology and service levels.
- Provided year-over-year reductions in the count and duration of outages through a high-touch service delivery experience, utilizing highly efficient processes and tools consistent with the IT Infrastructure Library (ITIL) and industry best practices.

Services

Event Management

Continuant will provide 24x7 event management that includes system monitoring and management of events for both TDM and UC equipment where applicable. Continuant will identify critical components in customers' environment and define key events for the specific system components. Continuant will provide structured levels of notifications to the customer for significant events detected in the customers' environment. Continuant Event Management will trigger Incident Management where applicable.

Incident Management

Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized. Continuant is responsible for prioritization and management of all incidents throughout their lifecycles.

Remote Incident Management

Remote Incident Management is provided 24/7 and ensures that normal service operation is managed through remote connectivity. Remote incident management activities may include remote diagnostics, troubleshooting, and remote support for onsite personnel. Activities may include:

- Resolve service disruptions and performance degradations on Managed Components.
- Manage incident escalations to ensure timely and high-quality resolution of all issues by monitoring time remaining to meet SLAs.
- Utilize Incident remediation procedures to collect any additional data required to diagnose and match to known errors in Continuant knowledge base.
- Remote labor to repair or replace a failed part or device and the subsequent testing to confirm correct operation of the device and its interface and operation with associated equipment, communication facilities and services.
- Remotely facilitate hardware replacement and software updates determined to be required by Continuant.
- Utilize and update Continuant's ITSM platform with relevant information relating to an Incident.
- Make an initial determination of the potential resolution.
- Resolve as many Incidents as possible during the Authorized User's initial contact with the Service Desk, without transferring the call or using any escalation.
- Resolve Incidents requiring Tier 1-3 Support and close the Incident after receiving confirmation from the affected Authorized User that the Incident has been resolved.
- Resolve Incidents arising from or related to the Services, including break/fix Hardware and Software support.
- Retain overall responsibility and ownership of all Incidents until the Incident is closed subject to Customer approval.
- Software support services – includes remote installation assistance and basic usability assistance on minor firmware, patches and bug fixes (all managed components must include Original Equipment Manufacturer (OEM) software support coverage when applicable). Software support services do not include the purchase of subscriptions that provide entitlement and rights to use future minor versions (point releases), future major releases of software, or patches.

Hardware Replacement

Continuant will provide hardware replacement on specified Covered Equipment. In the event of defective equipment, Continuant will make repairs or provide replacements of the defective equipment with either new equipment or a refurbished equivalent model at Continuant's discretion. Hardware Replacement includes parts within the telephone system (PBX) such as circuit packs, power supplies, processing elements and cabinetry, voicemail system (as applicable) and the primary server where a covered application resides. Telephone sets, power systems (UPS), PCs, servers, modems, routers, switches, wireless access points, security appliances, or other devices supporting carrier traffic are not included in this agreement unless specifically noted.

Change Management

Change Management is the process of assessing, controlling, managing and performing changes to a customer's infrastructure. The primary goal of this process is to ensure that changes are properly planned for, communicated, and approved. Change Management will consist of the following services:

- Continuant will follow the Request for Change (RFC) process. Providing the necessary documentation required to fulfill Change Requests. This will include associated plans required to implement the requested changes.

This process will be followed for Standard, Normal, and Emergency changes requested by the customer as agreed upon in this SOW. These changes are as follows:

- Standard – Standard changes are defined as well-known, repeatable and thoroughly documented procedures. These procedures present a low risk to operations and business services as determined by a standard risk assessment. Standard Changes are preauthorized by the Change Advisory Board to be implemented per terms agreed upon with the customer. If the Service owner is concerned about the risk and/or potential impact of a change on other services, then a Normal or Emergency change should be considered.

- Normal – Normal changes are defined as medium/high risk to business services and therefore must follow the normal change management process. Due to the potential risk and impact, normal changes must be reviewed, prioritized and scheduled by the Change Advisory Board (CAB). The Urgency of Normal Changes may be upgraded to accelerate the timeline for implementation given customer business justification of an impending business impact.

- Emergency – Emergency changes are defined as high risk to the business and required to be implemented as soon as possible – without proceeding through the normal change management process. They may be required to resolve a break/fix situation that has resulted in a service degradation or interruption in service. They may also be needed to

address an imminent interruption in service. Emergency Changes should leverage existing Standard Change procedures where applicable to reduce the associated risk. These Changes should also be related to a corresponding Incident where a service disruption or potential disruption has been recorded.

Service Desk

The Continuant Global Service Desk will be the primary communication point for services. The Customer will have several ways of interacting with the Global Service Desk. Customer Service Desk activities shall include the following:

- Perform initial analysis, troubleshooting, and diagnostics for Event Management
- Fulfill Service Requests for the “Customer”
- Provide proactive communication of service delivery
- Manage escalations to ensure timely and high-quality resolution
- Provide life-cycle management of all service requests and incidents
- Provide Technical Support for general advice and help on covered systems

Network Operation Center Services

While most support organizations provide a one-time network assessment, Continuant provides an on-going assessment to consistently monitor, enhance, and improve the Customer’s UC infrastructure.

- 24x7 event monitoring & management
- Perform initial analysis, troubleshooting, and diagnostics for Event Management

Technical Support

Continuant makes available to customers a dedicated team of engineers with OEM certifications to provide across-the-board Unified Communications Technical Support (TAC). TAC is designed to provide technical support for the customer when the customer has a question about their covered environment. Customer can access Continuant TAC when following the below guidelines and attributes:

- Command Instructions
- Terminology Definitions
- Programming/Configurational Vetting
- Does not require changes or programming
- Does not require onsite technical resources
- Does not require scheduled maintenance window
- Does not require discovery

- Can be completed in 15 minutes or less.

Continuant TAC will stop at 15 minutes. All work will be billed at current Time and Material rates that exceed 15 minutes. Continuant will advise the customer of the rates and obtain customer approval before providing further support.

Service Level Management

Continuant's Service Level Management (SLM) offering tracks performance against negotiated service level targets called Service Level Objectives (SLO). SLM is also responsible for ensuring that all operational service level agreements and underpinning contracts are appropriate. Continuant will monitor and report on service levels where applicable and provide reports according to an agreed upon schedule. Service Level Objectives (SLOs) apply only to components that are managed exclusively by Continuant within the service. Continuant adheres to the SLOs during the Service Delivery phase. Within the Customer Requirements Document, the Customer and Continuant must document their agreement to formally acknowledge the completion of the Service Transition process. The Service Delivery phase commences upon mutual agreement between Continuant and the Customer that the Service Transition phase is complete and that the Service Delivery phase has been reached.

The following metrics are tracked as SLOs:

- Time to Notify (TTN)
- Time to Restore (TTR)
- Time to Complete (TTC)

Incident Prioritization: Continuant classifies and prioritizes incidents according to Impact and Urgency. Continuant will evaluate Incident Impact and Urgency to classify all Incidents into Priority 1 (P1), Priority 2 (P2), Priority 3 (P3) and Priority 4 (P4) Incident categories.

Continuant Incident Management Priorities Matrix

	Impact			
Urgency	Widespread	Large	Localized	Individualized
Critical	P1	P1	P2	P2
High	P1	P2	P2	P3
Medium	P2	P3	P3	P3
Low	P4	P4	P4	P4

Exhibit 2

Impact Definitions: An Incident is classified according to its impact on the business (the size, scope, and complexity of the Incident). Impact is a measure of the business criticality of an Incident, often equal to the extent to which an Incident leads to degradation of a Service. Continuant will work with Customer to specify Impact for each Managed Component during Service Transition. There are four Impact levels:

- **Widespread** – Entire Network is affected (more than three quarters of individuals, sites or devices)
- **Large** – Multiple sites are affected (between one-half and three-quarters of individuals, sites or devices)
- **Localized** – Single site, room and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)
- **Individualized** – A single user is affected (less than one-quarter of individuals, sites or devices)

Urgency Definition: Urgency defines the criticality of the Incident to Customer's business. Continuant will work with Customer to understand and set the proper Urgency level. There are four Urgency levels:

- **Critical** – Primary business function is stopped with no redundancy or backup. There may be an immediate financial impact to Customer's business.
- **High** – Primary business function is severely degraded or supported by backup or redundant system. There is potential for a significant financial impact to Customer's business.
- **Medium** – Non-critical business function is stopped or severely degraded. There is a possible financial impact to Customer's business.
- **Low** – Non-critical business function is degraded. There is little or no financial impact.

Time to Notify (TTN)

Customers may have specific notification requirements for which the Service will offer a Time to Notify (also known as "Respond") objective. Continuant will respond to incidents and requests raised through the management platform by electronically notifying a specified Customer contact(s) within the TTN timeframe. Continuant SLAs are as follows:

Case contact method	*Continuant estimated time to notify to specified contact*	*Incident or Service Request Level*	*SLO Target*
Event Managements Cases	15 Minutes from event opened date/time	All priority incidents	95%
Phone Call from “Customer”	15 Minutes from call being answered	All priority incidents and service requests	95%
Email from “Customer” to Service Desk	15 Minutes from email received date/time	All priority incidents and service requests	95%
Continuant Service Portal	15 Minutes from case opened date/time	All priority incidents and service requests	95%

Time to Restore (TTR)

Incidents go through many stages, with restoration being a primary objective. Time to Restore tickets includes all remote incident management activities (alarm or call receipt through restore, excluding maintenance or carrier cycle time). TTR refers to the time elapsed between the failure which caused the incident and when Continuant restores the managed component to an acceptable operational state. Continuant SLAs for meeting this objective are as follows:

Incident Level	*Time to Restore*	*SLO Target*
P1 Incidents	4 Hours	95%
P2 Incidents	12 Hours	95%
P3 Incidents	72 Hours	95%
P4 Incidents	120 Hours	95%

SLO measurements exclude the following:

- Delays caused by Customer in resolving the qualifying issue (for example, waiting for response on change window or on-site resources).
- Any mutually agreed upon schedule of activities that causes service levels to fall outside of measured SLOs defined obligations.
- SLOs will be paused for hardware replacement delivery to the customer location, either from a manufacturer maintenance agreement or hardware replacement services from Continuant.
- Delays or faults caused by third party equipment, services or vendors, such as Carriers, in resolving the qualifying issue.
- Other factors outside of Continuant's reasonable control for which Continuant is not responsible.
- Acquisition and installation time of new software to be installed on the Managed Component due to software defects or bugs.

Time to Complete (TTC)

Continuant has categorized requests based on level of risk, complexity and the amount of time required to complete the request. All Changes are scheduled events and are dependent on coordination with Customer's schedule. A change request must be fully qualified and scheduled with Customer before the Time to Complete metric starts. All custom requests for change are scheduled events and follow the Normal Change Management procedures.

The chart below provides a breakdown of the available categories and durations for three types of requests.

Continuant SLOs for completing requests are as follows:

Change Request	*Time to completion from receipt of fully qualified and scheduled change request*	*SLO Target*
Remote Simple	2 business days	95%
Remote Simple – Expedited	8 hours	95%
Complex	Within 5 business days*	95%

Exhibit 2

Project	No SLO, scheduled	No SLO

**SLO time commences upon Continuant receiving signed quote from Customer.*

**Enhanced entitlements are available at a premium.*

SLO measurements exclude the following:

- Delays caused by Customer in executing the requested change (for example, waiting for response on change window).
- Any mutually agreed upon schedule of activities that causes service levels to fall outside of measured SLAs defined obligations.
- Other factors outside of Continuant's reasonable control for which Continuant is not responsible.
- Ticket closure time may be different than change completion time. For example: a ticket may be kept open for review after the change has been executed.

Any Customer-requested changes that are considered by the Customer as "emergency" or "urgent" changes will be treated on a commercially reasonable effort by the Continuant Service Desk and will depend on Continuant engineer availability at the time of submittal. Additional charges may apply.

Additional Managed Services

*Only applies to Optional MAP Services listed on page 1 of this Scope of Work with YES in the "Selected" column.

24/7 Onsite Incident Management

Continuant will provide 24/7 onsite support that ensures normal Service Operation is restored as quickly as possible and the business impact is minimized through the dispatch of local technicians. Activities may include 24/7 dispatch of local technicians for diagnostics, troubleshooting, and/or parts replacement (parts not included, unless they are covered under Hardware Replacement Services). The Customer is responsible for providing access to the site.

Other Information

Continuant Remote Access and Monitoring Platform

The Continuant-owned Secure Access Server (SAS) will allow remote access and monitoring for all managed systems supported by Continuant. The SAS contains all management software and hardware required for the delivery of services. The SAS is securely deployed on the Customer's network in a single configuration instance or multiple instance configurations depending on the number, type, and location of the managed components. During the coverage term, Customers are granted a nonexclusive and nontransferable license to use the hardware and the software resident solely on the SAS supplied by Continuant. Customers must return any and all associated SAS materials and connectivity devices to Continuant immediately upon expiration or termination of the agreement. Any delay by the Customer with supporting these Remote Access requirements may result in time and material charges for maintenance services. The Continuant SAS security compliance documentation is available upon request.

Asset Management

Continuant's Asset Management standard service will use the Service Activation Kit (SAK) information listed in the Customer Responsibilities section below to capture specific information for the Covered Equipment that includes the following:

- Serial Number
- Model Number
- System Firmware\Operating version
- Physical Location to include;
  - Street Address,
  - Floor Number
  - Room Number
  - Rack Location (if Applicable)
  - Brief description of the location
- Credentials for accessing and resolving issues with the equipment (May require top level admin/root)

Customer Responsibilities

The Customer is responsible for completing a Service Activation Kit (SAK), which provides Continuant the key information critical to success for commencement of maintenance. The Customer will complete tasks defined in the SAK to enable management access to Covered Equipment which may include setting up SNMP traps, and system logs. These activities are both critical and beneficial to the Customer and Continuant as these activities establish a managed connection required for Continuant to resolve incidents and service requests quickly.
Items in the SAK include:

- Customer representative contact name
- Location of the site(s) to be managed
- Location of management applications
- Network connectivity approval and placement detail for the SAS
- Device location and naming scheme
- Management IP addresses and system detail, SNMP community strings
- Access method and credentials (Telnet, Remote Desktop, etc.)

- Management system User names and contact detail
- Installation of the SAS and network connectivity per Continuant-supplied guidelines.
- Communications facilities and services including internet and network configuration. The communication facilities and services must be maintained for the duration of the service term.
- Resource to support the installation activities of the SAS, which may include:
  - Racking
  - Connection to Network
  - Power connection to UPS or other facility with continuous uninterrupted power
  - Provide suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the SAS.

**Any delay or error by the customer in providing this information could delay commencement date.*

Location & Covered Equipment

Location Name	*Services & Equipment*	*Paid Monthly*	*Paid Annually*
Blume Road/Engineering • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 19 – 51 user(s) Avaya PBX Base Plan • Media Gateway 19 – 51 user(s)	$ 70.38	$ 844.56
Dairy Ashford • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 8 – 9 user(s) Avaya PBX Base Plan • Media Gateway 8 – 9 user(s)	$ 50.00	$ 600.00
Emily Court • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 9 – 7 user(s) Avaya PBX Base Plan • Media Gateway 9 – 7 user(s)	$ 50.00	$ 600.00
Extension Services • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 13 – 91 user(s) Avaya PBX Base Plan • Media Gateway 13 – 91 user(s)	$ 125.58	$ 1,506.96
JP Needville • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 20 – 18 user(s) Avaya PBX Base Plan • Media Gateway 20 – 18 user(s)	$ 50.00	$ 600.00
Jane Long (Main) • DOC: 10/01/2021	Small Server Support • System Manager – 1 server(s) 24/7 Onsite Incident Management • Avaya CMS – 30 agent(s) • System Manager – 1 server(s) • ESS – 1 server(s) • Session Manager – 2 server(s) • Avaya Aura Messaging – 1,478 user(s) • Avaya CM 6.3 – 1,727 user(s) Avaya VM Base Plan • Avaya Aura Messaging – 1,478 user(s) Avaya PBX Base Plan • Avaya CM 6.3 – 1,727 user(s) Contact Center Per User (1 - 49 users) • Avaya CMS – 30 agent(s) Large Server Support (CSS) • ESS – 1 server(s) • Session Manager – 2 server(s)	$ 3,369.30	$ 40,431.60
Justice Center • DOC: 10/01/2021	24/7 Onsite Incident Management	$ 142.14	$ 1,705.68

Location Name	Services & Equipment	Paid Monthly	Paid Annually
	• Media Gateway 1, 2 – 103 user(s) Avaya PBX Base Plan • Media Gateway 1, 2 – 103 user(s)		
Juvenile • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 17 – 112 user(s) Avaya PBX Base Plan • Media Gateway 17 – 112 user(s)	$ 154.56	$ 1,854.72
Needville R&B • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 12 – 24 user(s) Avaya PBX Base Plan • Media Gateway 12 – 24 user(s)	$ 50.00	$ 600.00
PCT (precinct) 1 • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 3 – 29 user(s) Avaya PBX Base Plan • Media Gateway 3 – 29 user(s)	$ 50.00	$ 600.00
PCT (precinct) 2 • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 7 – 29 user(s) Avaya PBX Base Plan • Media Gateway 7 – 29 user(s)	$ 50.00	$ 600.00
PCT (precinct) 3 • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 15 – 30 user(s) Avaya PBX Base Plan • Media Gateway 15 – 30 user(s)	$ 50.00	$ 600.00
R&B Beechnut • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 16 – 20 user(s) Avaya PBX Base Plan • Media Gateway 16 – 20 user(s)	$ 50.00	$ 600.00
R&B Crabb • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 14 – 46 user(s) Avaya PBX Base Plan • Media Gateway 14 – 46 user(s)	$ 63.48	$ 761.76
Rosenberg Annex • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 18 – 143 user(s) Avaya PBX Base Plan • Media Gateway 18 – 143 user(s)	$ 197.34	$ 2,368.08
Rosenberg Bootcamp • DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 21 – 13 user(s) Avaya PBX Base Plan • Media Gateway 21 – 13 user(s)	$ 50.00	$ 600.00
Tax Office			

Location Name	Services & Equipment	Paid Monthly	Paid Annually
• DOC: 10/01/2021	24/7 Onsite Incident Management • Media Gateway 11 – 60 user(s) Avaya PBX Base Plan • Media Gateway 11 – 60 user(s)	$ 82.80	$ 993.60