State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA STATEWIDE CONTRACT WITH CELONIS, INC.

This State of Oklahoma Statewide Contract No. 1041 ("Contract") is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services ("State") and Celonis, Inc. ("Supplier") and is effective as of the date of last signature to this Contract. The initial Contract term, which begins on the effective date of the Contract, will run concurrently with award dated 03/14/2023. There will be four (4) annual optional renewals remaining.

Purpose

The State is awarding this Contract to Supplier for the provision of certain software and services to support State agencies and other eligible Oklahoma Interlocal Entities, which may include the following: software, training, pre-sales assistance, documentation, implementation, maintenance, support, configuration, as more particularly described in certain Contract Documents. This Contract memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.

2. The following Contract Documents are attached hereto and incorporated herein:

   2.1 Solicitation 0000000199, Attachment A;
   2.1. General Terms, Attachment B;
   2.2. Oklahoma Statewide Contract terms, Attachment C;
   2.3. Information Technology terms, Attachment D;
   2.4. Information Security Requirements, Attachment D-1;
   2.5. Pricing, Attachment E-1
   2.6. Service Level Agreement, Attachment E-2
   2.7. Celonis End User Master Service Agreement, Attachment E-3
   2.8. Support Services Description, Attachment E-4

2.9. Metrics Description EMS, Attachment E-5

2.10. Product EMS Description, Attachment E-6

2.11. Negotiated Exceptions to Contract, Attachment F; and

2.12. Template for Contract Modifications for Quotes, Statements of Work, or other Ordering Documents, Attachment F-1.

3. The parties additionally agree:

3.1 Except for information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

3.2 Unless mutually agreed to in writing by the State's Chief Information Officer utilizing Attachment F-1 and Supplier, no Contract Document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator, shall supersede or conflict with the terms of this Contract or expand the State's or Customer's liability or reduce the rights of Customer or the State. The parties agree and understand that Supplier will not be acting as a reseller under this Contract.

3.3 To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the parties make no representation or warranty regarding the enforceability of such term or condition and the parties do not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.

3.4 **Geographic Limits.** Customer Data will be hosted within the geographic limits of the United States of America ("US"), and Supplier will not otherwise create, transmit, receive, access, process, store, or maintain Customer Data outside the geographic limits of the US, unless otherwise permitted per the Geographical Restriction Exceptions listed below or upon the State's prior written authorization. Under no circumstances will Customer Data be hosted outside the US. The parties additionally agree that all Support Services and Professional Services, where applicable, will be performed within the US, except as otherwise agreed to by the State. To the extent offshore resources are needed in the performance of Support Services or Professional Services, it will be addressed in the associated statement of work, work order, order form or other similar ordering document and require prior notice and written approval by the State. With the exception of the Geographical Restriction Exceptions set forth below, Supplier agrees to follow the Offshore Data Storage Standard found at Offshore Data Storage Standard (oklahoma.gov).

3.4.1 **Geographical Restriction Exceptions**

(1) Support Ticketing Requests. As of the Effective Date, the State acknowledges that all support ticketing requests relating to the Services (each, a “Support Request”) will be made through Supplier’s support ticketing system operated in Munich, Germany from a server environment used by Supplier through its third-party subcontractor, Salesforce.com Germany GmbH. Notwithstanding anything to the contrary hereunder, Supplier shall not be considered in breach of the Contract in the event that the State includes or shares its Customer Data in the process of creating and submitting any Support Request.

(2) Operational Data/R&D Efforts. Furthermore, notwithstanding anything to the contrary hereunder, the following shall not be subject to geographical limited or restrictions: a) operational data related to the Supplier’s Cloud Service (such as log files, application-related usage data or other infrastructure-related information), and b) Supplier’s and/or its agents’ engineering and research and development efforts related to the Cloud Service.

(3) Employee Access Via Email. Notwithstanding anything to the contrary hereunder, Supplier shall not be considered in breach of the Contract in the event that the State includes or shares its Customer Data via email or other electronic communication (i.e., instant messaging, video conferencing tools, shareable/collaborative online tools) and such Customer Data is then accessed, reviewed or otherwise processed by a Supplier employee who is outside of the US. Any such Customer Data shall be held in accordance with the confidentiality provisions set forth under the Contract. Any additional documents provided by Supplier in their bid response that are not included in this final Contract have been rejected by the State and are not intended to be part of this final Contract.

Attachments referenced in this section are attached hereto and incorporated herein.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA by and through the OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES

By: Joe McIntosh (Jun 21, 2024 10:02 CDT)

Name: Paul J. McIntosh

Title: Chief Information Officer

Date: 06/21/2024

Celonis, Inc.

By: DocuSigned by: Marya Milton 03F7E1F8AE014B7...

Name: Marya Milton

Title: VP & AGC

Date: Jul 1, 2024 | 8:19 PM CEST

ATTACHMENT A
EVENT NO. 0000000199

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services for software and services to support State agencies and other eligible Oklahoma Interlocal Entities. This Supplier will provide software, training, pre-sales assistance, documentation, installation, maintenance, support, configuration, customization, and license agreement administration. This bid supports both SaaS Cloud Based Solutions and On-Prem Software Solutions.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, will run concurrently with award dated 03/14/2023. There will be four (4) annual renewals remaining.

This RFP is a supplemental solicitation to Solicitation 0900000556 to add additional suppliers within scope.

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms ("General Terms") is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

1.1 Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2 At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3 If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

1.4 The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

1.5 Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

2.1 Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

2.2 Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

A. any Addendum;

B. any applicable Solicitation;

C. any Contract-specific State terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

D. the terms contained in this Contract Document;

E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;

F. any statement of work, work order, or other similar ordering document as applicable; and

G. other mutually agreed Contract Documents.

2.3 If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 Modification of Contract Terms and Contract Documents

3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 Definitions

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2 **Addendum** means a mutually executed, written modification to a Contract Document.

4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.

4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.

4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.

4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.

4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.

4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

4.14 **OAC** means the Oklahoma Administrative Code.

4.15 **OMES** means the Office of Management and Enterprise Services.

4.16 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

4.17 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

4.18 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.

4.19 **Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.

4.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

4.21 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

5.1 Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.

5.2 Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.

5.3 The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

6.1 Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

6.2 Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.

6.4 Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

7.1 Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

A. An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.

B. Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.

C. Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D. The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.

E. If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.

F. Supplier shall have no right of setoff.

G. Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.

H. The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

8.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than $5,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $5,000,000 combined single limit each accident;

D. Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than $5,000,000 per occurrence;

E. Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits $5,000,000 per occurrence; and

F. Additional coverage required in writing in connection with a particular Acquisition.

8.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

8.3 Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

9.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:

A. Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B. Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;

C. Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;

D. 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;

E. Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;

H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at **www.dhs.gov/E-Verify**;

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at **Information Security Policy, Procedures, Guidelines (oklahoma.gov)**. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.

9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source.

9.5 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.

9.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

9.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.

9.8 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.

9.9 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

9.10 If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

10.1 As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

10.2 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

10.3 Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

11.1 The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer's prior express written permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

11.2 Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.

11.3 Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

13.1 Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

13.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3 If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property, copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

A. Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

B. To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B. Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

17.1 Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.

17.3 The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

18.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.

18.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

18.3 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

19.1 The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

19.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

20.1 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

20.2 Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

20.3 Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:
State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq*. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

A. No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B. The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C. The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.

D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

1.1 The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.

1.2 The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

2.1 Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.

2.2 Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.

2.3 Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

i. Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov;

ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;

iii. Submission no later than forty-five (45) days following the end of each calendar quarter;

iv. Contract quarterly reporting periods shall be as follows:

a. January 01 through March 31;

b. April 01 through June 30;

c. July 01 through September 30; and

d. October 01 through December 31.

v. Reports must include the following information:

a. Procuring entity;
b. Order date;

c. Purchase Order number or note that the transaction was paid by Purchase Card;

d. City in which products or services were received or specific office or subdivision title;

e. Product manufacturer or type of service;

f. Manufacturer item number, if applicable;

g. Product description;

h. General product category, if applicable;

i. Quantity;

j. Unit list price or MSRP, as applicable;

k. Unit price charged to the purchasing entity; and

l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms ("Information Technology Terms"), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services ("OMES-IS") is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

1.1 **COTS** means software that is commercial off the shelf.

1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.

1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.

1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.

1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

1.8 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

1.9 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.

1.10 **State CIO** means the State Chief Information Officer or authorized designee.

1.11 **Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

1.12 **Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.

1.13 **Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to- practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

2.1 Customer removes the product for which the services are provided, from productive use or;

2.2 The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/accessibility-standards.html. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required, and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

6.1 The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at [Information Security Policy, Procedures, Guidelines (oklahoma.gov)]

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards.html

6.2 Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other applicable Customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State.

9 Source Code Escrow

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

9.1 A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;

9.2 An assignment by the Supplier for the benefit of its creditors;

9.3 A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;

9.4 The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;

9.5 The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;

9.6 The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;

9.7 Supplier's ceasing of maintenance and support of the software; or

9.8 Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as “Work for Hire”, Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

12.1 As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered “works made for hire” and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.

12.2 Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier’s signature due to the dissolution of Supplier or Supplier’s failure to respond to Customer’s repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier’s agent and Supplier’s attorney-in-fact to act for and in Supplier’s behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer’s sole expense, in the preparation and prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

12.3 Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.

12.4 All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.

12.5 These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.

12.6 Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.

12.7 Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.

12.8 To the extent that any Third-Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer’s internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third-Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third-Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer’s internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party’s written approval for Supplier to use any Third-Party Intellectual Property that may be embodied or reflected in the Work Product.

12.9 Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.

12.10 To the extent not inconsistent with Customer’s rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.

12.11 If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 Hosting Services

13.1 If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:
Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.

3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.

4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.

5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

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

7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. **Security Incident or Data Breach Notification:** Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.

2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).

3. Supplier shall:

a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;

b. Make summary information regarding such procedures available to Customer at Customer's request;

c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

2. Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. **Notices**

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to:

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

3. Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5. Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices "A" & "B";

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist		Compliance checklist –
Policy Area 1	Information Exchange Agreements	
Policy Area 2	Security Awareness Training	
Policy Area 3	Incident Response	
Policy Area 4	Auditing and Accountability	
Policy Area 5	Access Control	
Policy Area 6	Identification and Authentication	
Policy Area 7	Configuration Management	
Policy Area 8	Media Protection	
Policy Area 9	Physical Protection	
Policy Area 10	Systems and Communications Protection and Information Integrity	
Policy Area 11	Formal Audits	
Policy Area 12	Personnel Security	

Attachment D-1
Information Security Requirements

1. General Information Security Requirements

a. No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.

b. Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.

c. Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.

d. Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

2. HIPAA Requirements

a. Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).

b. If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse, and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.

c. <u>Business Associate Terms Definitions</u>:

   i. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business

Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

ii. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.

iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.

iv. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.

v. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

d. Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:

i. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;

ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

iii. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;

iv. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;

v. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);

vi. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;

vii. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

viii. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;

ix. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;

x. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual who's Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;

xi. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;

xii. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;

xiii. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;

xiv. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;

xv. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and

xvi. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

e. Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:

i. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;

ii. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;

iii. disclose PHI to report violations of law to appropriate federal and state authorities; or

iv. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

v. make uses and disclosures and requests for protected health information consistent with Covered Entity’s minimum necessary policies and procedures;

vi. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].

f. Obligations of Covered Entity

i. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate’s use or disclosure of PHI.

ii. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of protected health information.

iii. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.

iv. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.

v. Covered Entity shall provide the minimum necessary PHI to Business Associate.

g. Term and Termination:

i. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:

(1) retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(2) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;

(3) continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

(4) not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under “Permitted Uses and Disclosures By Business Associate” that applied prior to termination; and

(5) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

ii. All other applicable obligations of Business Associate under this Agreement shall survive termination.

iii. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

h. Miscellaneous Provisions:

i. No Third Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

ii. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.

iii. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.

iv. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.

v. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.

vi. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.

vii. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

3. **42 C.F.R. Part 2 Related Provisions**

a. Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

i. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;

ii. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of an kind;

iii. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;

iv. Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

v. Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

vi. Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;

vii. Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;

viii. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

ix. Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.

b. Data Security. The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.

c. Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.

d. Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.

e. Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

4. Federal Tax Information Requirements IRS Publication 1075 (If Applicable)

a. PERFORMANCE: If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

i. All work will be performed under the supervision of the State of Oklahoma.

ii. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

iii. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

iv. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

v. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

vi. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

vii. All Contractor computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

x. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

xi. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

xii. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

b. CRIMINAL/CIVIL SANCTIONS

i. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

ii. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

iii. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

iv. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

v. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

c. INSPECTION: The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

5. SSA Requirements (If applicable)

a. PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:

i. All work will be done under the supervision of the State of Oklahoma.

ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.

iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.

v. The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.

vi. Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.

vii. Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

viii. Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.

ix. The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.

x. Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.

xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

xiii. If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

xiv. In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.

xv. The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

b. CRIMINAL/CIVIL SANCTIONS: The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

i. Civil Remedies.

(1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of —

(a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of $1,000; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

(2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where

parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(1).

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(2).

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(3).

6. Child Support FPLS Requirements (If applicable)

a. Contractor, when applicable and to the extent within Contractor’s control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.

ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

7. **FERPA Requirements (If applicable)**

a. If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

8. **CJIS Requirements (If applicable)**

a. INTRODUCTION

This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

b. CJIS SECURITY POLICY REQUIREMENTS GENERALLY
The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."

c. DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices "A" & "B";

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices "D", "E", "F" & "H"; and
5. the Supplemental Guidance in Appendices "J" & "K".

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

ATTACHMENT E-1 to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199

The Pricing is hereby amended to include the terms as set forth below and supersedes all prior Pricing submitted by Celonis or discussed by the parties.

SW1041 Software-Supplemental

Software Publishers			
Description	Part Description	Maximum Cost + % Markup	% off List Price
EMS for Public Sector Small Cities/Counties	Includes 1 EMS Team, 20 APC, 5 Business Users, 1 Analyst, 150,000 Executions (annual term)	$50,000.00	2.00%
EMS for Public Sector Federal/State Agencies	Includes Unlimited Business Users, Unlimited Analysts, 1 concurrent process (annual term)	$500,000.00	2.00%
Celonis Process Mining for Public Sector - High Control Edition	Includes: 1 Concurrent Process, Unlimited Named Users (annual term)	$300,000.00	2.00%
24x7 Premium Support - Tier 1	24 X 7 Support (annual term)	$50,000.00	2.00%
24x7 Premium Support - Tier 2	24 X 7 Support (annual term)	$100,000.00	2.00%
24x7 Premium Support - Tier 3	24 X 7 Support (annual term)	$150,000.00	2.00%
24x7 Premium Support - Tier 4	24 X 7 Support (annual term)	$200,000.00	2.00%
24x7 Premium Support - Tier 5	24 X 7 Support (annual term)	$250,000.00	2.00%
Premium Sandbox - Tier 1	EMS platform add-on, 1 Premium Sandbox EMS Team (for non-productive usage and testing purposes only), with Analysts (no Business Users), Executions and APC as per the Customer's productive EMS Team(s), (Annual term)	$75,000.00	2.00%
Premium Sandbox - Tier 2	EMS platform add-on, 1 Premium Sandbox EMS Team (for non-productive usage and testing purposes only), with Analysts (no Business Users), Executions and APC as per the Customer's productive EMS Team(s), (Annual term)	$150,000.00	2.00%
Premium Sandbox - Tier 3	EMS platform add-on, 1 Premium Sandbox EMS Team (for non-productive usage and testing purposes only), with Analysts (no Business Users), Executions and APC as per the Customer's productive EMS Team(s), (Annual term)	$225,000.00	2.00%
Premium Sandbox - Tier 4	EMS platform add-on, 1 Premium Sandbox EMS Team (for non-productive usage and testing purposes only), with Analysts (no Business Users), Executions and APC as per the Customer's productive EMS Team(s), (Annual term)	$300,000.00	2.00%
Premium Sandbox - Tier 5	EMS platform add-on, 1 Premium Sandbox EMS Team (for non-productive usage and testing purposes only), with Analysts (no Business Users), Executions and APC as per the Customer's productive EMS Team(s), (Annual term)	$375,000.00	2.00%
ML Workbench, dedicated resource, standard	EMS platform add-on, Standard instance includes 16 vCPU, 128 GB RAM, 200 GB Disk Space. (Monthly Rate)	$5,570.00	2.00%
Additional Business User, per named user	EMS platform additional business user (annual term)	$2,000.00	2.00%
Additional Analyst, per named user	EMS platform additional analyst user (annual term)	$4,000.00	2.00%
Additional APC, per GB	EMS platform additional APC (annual term)	$1,400.00	2.00%
Additional Executions, per execution / year	EMS platform additional executions (annual term)	$0.12	2.00%

Other Value Add Products and Services			
Description	Part Description	Maximum Cost + % Markup	% off List Price

Professional Services - Hourly Not-to-Exceed Rates			
Description	Part Description	List Price	Discounted Hourly Rates
Proof of Value	Flat fee for proof of value customer engagement (flat fee)	$7,500.00	0.00%
Service Team Resource	Service Team Resources, per Consultant Day (per day)	$2,360.00	0.00%
Master Class	Participation Fee for one individual to attend a single stream of the Celonis Master Class.	$1,850.00	0.00%
Classroom Training at Celonis Training Center	Classroom training hosted in one of the Celonis training centers, including preparation.	$600.00	0.00%
Onsite Training Instructor-led (Hour)	At the customer site, including preparation, maximum 10 participants per training. 1 hour.	$350.00	0.00%
Certification Exam Volume Bundle (S)	Users using the voucher are granted a non-exclusive, non-transferable right to access the Celonis Training Platform to complete the certification exam. 25 Registrations	$3,150.00	0.00%
Solution Creation Expert Bundle	Users using the voucher are granted a non-exclusive, non-transferable right to access the Celonis Training Platform to complete the specified certification exams (3 in total).	$380.00	0.00%
Value Assessment Expert Bundle	Users using the voucher are granted a non-exclusive, non-transferable right to access the Celonis Training Platform to complete the specified certification exams (3 in total).	$380.00	0.00%
EMS Technical Expert Bundle	Users using the voucher are granted a non-exclusive, non-transferable right to access the Celonis Training Platform to complete the specified certification exams (5 in total).	$635.00	0.00%
Value Realization Expert Bundle	Users using the voucher are granted a non-exclusive, non-transferable right to access the Celonis Training Platform to complete the specified certification exams (4 in total).	$510.00	0.00%
Certification Exam (Individual Purchase)	Users purchasing this product directly in the Celonis Academy are entitled to 2 attempts to pass the chosen online certification exam.	$150.00	0.00%

celonis

ATTACHMENT E-2 to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199

The Service Level Agreement is hereby amended to include the terms as set forth below and supersedes all prior Service Level Agreements submitted by Celonis, Inc. or discussed by the parties. The terms and conditions of SW1041 prevail over any conflicting terms and conditions in this document.

Service Level Agreement

For Celonis Cloud Service Offerings

Celonis Execution Management System enables you to see how your business processes have been executed. Due to the transparency provided by Celonis Execution Management System, the success of optimization measures can be reviewed at once. Moreover, process patterns and metrics can be analyzed and continuously monitored.

1. Cloud Service Uptime

We will use commercially reasonable efforts to provide you access to the Cloud Service of the Celonis Execution Management System on a twenty-four hour, seven days a week (24x7) basis at an uptime rate of 99.5 % calculated monthly.

Cloud Service Uptime Measurement

The Cloud Service Uptime will commence to be measured on our mutually agreed to-be determined go-live date, which shall in no event be prior to the actual go-live date. The actual "Go-Live Date" shall be the date on the following conditions have been met: (i) we have for the first time provided access to the Cloud Service in the production environment; (ii) end-user testing is completed by you and us; and (iii) you can access the production environment with production data for the first time.

However, we may not be able to guarantee the uptime rate in some cases. Thus, the Cloud Service Uptime Measurement shall not apply to performance issues caused by the following:

- ✓ Overall internet congestion, slowdown, or unavailability
- ✓ Unavailability of generic internet services (e.g. DNS servers)
- ✓ Virus or hacker attacks
- ✓ Force majeure events
- ✓ Actions or inactions of you or third parties beyond our control
- ✓ A result of your equipment or third-party computer hardware, software, or network infrastructure not within our control
- ✓ Scheduled SaaS infrastructure maintenance (see below)

2. System Uptime Report

Upon your request, we will provide you with a Cloud Service Uptime Report. Each Cloud Service Uptime Report will cover a period of twelve (12) months, measured backwards from the end of the calendar month that preceded the date of the request. If you do not agree with the SaaS Uptime Metric Report, written notice of the dispute must be provided to us within fifteen (15 days) of receipt of the Cloud Service Uptime Report.

3. Scheduled Infrastructure Maintenance

Scheduled Maintenance times for the Celonis Software will be posted on the *status.celonis.com*. We endeavor to provide at least forty-eight hours prior posting of any scheduled maintenance for the Celonis Software. In addition, updates will be uploaded to the SaaS infrastructure approximately four times per year. This may cause short breaks in the availability of the service as well. We will inform You about such updates in advance.

ATTACHMENT E-3 to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199

The Celonis Government End User Master Services Agreement is hereby amended to include the terms as set forth below and supersedes all prior Celonis Government End User Master Services Agreements submitted by Celonis or discussed by the parties.

Celonis Government End User Master Services Agreement

IF YOU HAVE A SEPARATE, SIGNED AGREEMENT GOVERNING YOUR USE OF THE SERVICES (STATEWIDE CONTRACT NO. 1041), THE TERMS AND CONDITIONS OF SUCH OTHER AGREEMENT, STATEWIDE CONTRACT NO. 1041, SHALL PREVAIL OVER ANY CONFLICTING TERMS OR CONDITIONS IN THIS AGREEMENT. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, SUCH INDIVIDUAL REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERM "YOU" SHALL REFER TO SUCH ENTITY. THIS AGREEMENT IS EFFECTIVE AS OF THE EARLIER OF (A) THE EFFECTIVE DATE OF THE FIRST ORDER REFERENCING THIS AGREEMENT, OR (B) AS OF YOUR INITIAL ACCESS TO THE SERVICE ("**EFFECTIVE DATE**"). Celonis agrees and understands that any definitions, terms or condition identified in Statewide Contract No 1041 prevail over any conflicting definitions, terms or condition, including any hyperlinks, contained in this Celonis Government End User Master Services Agreement. Further, to the extent any terms and conditions within this Celonis Government End User Master Services Agreement, including via any embedded hyperlinks, violate State or Federal law, the State does not agree to any such terms.

1. **Definitions.** All definitions not defined in the main body of this Agreement are specified in Annex A.

2. Agreement.

2.1 This Agreement governs Your access to and use of the Services specified in the applicable Order or purchased by You via an online platform. This Agreement will commence on the Effective Date and continue until the earlier of: (i) termination for cause in accordance with Section 13, or (ii) expiration of all Orders under this Agreement.

3. Our Obligations.

3.1 During the Subscription Term, and subject to the terms and conditions of this Agreement and any limitations specified in an Order (STATEWIDE CONTRACT NO. 1041), We shall: (i) make the Services available to You in accordance with the Documentation and Service Level Agreement, (ii) provide Support Services in accordance with the Support Services Description, and (iii) provide the Professional Services as further described in each Order.

3.2 We are solely responsible for all matters relating to the payment of Our employees and contractors, including without limitation providing compensation and other benefits such as vacation or sick pay, social security, medical care, unemployment or disability insurance, worker's compensation, health and welfare benefits, profit sharing, retirement/pension, or any employee stock option or stock purchase plans and complying with all other federal, state and local laws, rules and regulations governing such matters.

4. Rights of Access and Your Obligations.

4.1 Subject to the terms of this Agreement, and except as otherwise permitted in the Documentation, during the Subscription Term, You may enable User access to and use of the Services solely for Your internal business purposes in accordance with the limitations specified in the Metrics Definition and not for the benefit of any third parties. Your third-party suppliers or contractors may access and use the Services for the sole purpose of providing their goods and/or services to You. You will be entitled to copy the Documentation and materials accompanying the Service as may reasonably be required for Your internal purposes.

4.2 You shall: (i) be responsible for Your Users' compliance with this Agreement, the Documentation and any use limitations specified in the applicable Order or online purchasing portal; (ii) use commercially reasonable efforts to prevent any unauthorized access to or use of the Services and promptly notify Us in the event of any such unauthorized access or use; (iii) have sole responsibility for the accuracy, quality, and legality of all Customer Data and Customer Materials; (iv) be solely liable for uploading Customer Data and making appropriate backups of such Customer Data; (v) obtain any legally-necessary consents and/or provide required privacy notices to any party whose Personal Data you input into the Service or otherwise provide Us; (vi) cooperate with Us on any matters relating to the Professional Services as set out in the Order and provide Us with prompt feedback to Our requests; and (vii) in the event Professional Services are provided on Your premises, provide Us with safe and adequate space, power, network connections, materials, CPU time, access to hardware, software and other equipment and information, and assistance from qualified personnel as We may reasonably request from time to time.

4.3 In connection with this Agreement, You shall not: (i) use the Services for the benefit of anyone other than Yourself or Your Affiliates, unless expressly stated otherwise in an Order or the Documentation; (ii) send, store or transfer infringing, obscene, threatening, libelous or otherwise unlawful or tortious material, including material that violates privacy rights or third-party Proprietary Rights; (iii) upload, input, access, store, distribute or transmit any Malware; (iv) except as specified in the Documentation, modify, copy, translate or create derivative works based on a Service or any part, feature, function or user interface thereof; or (v) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the Services to build a competitive product or service or one with similar ideas, features, functions or graphics or to determine whether the Services are within the scope of any patent.

4.4 Any use of the Services in breach of this Section 4 may result in: (i) termination for breach in accordance with Section 13, or (ii) the immediate temporary suspension of the Services if We have a reasonable, articulable suspicion that such use threatens the security, integrity or availability of the Services. We shall promptly notify You of any such suspension and provide the justification therefor. Where reasonable to do so, We shall (a) provide such notification in advance and (b) work with You in good faith to cure the breach prior to suspending Your access. Any suspension will be limited to the scope and duration reasonably required to eliminate the threat identified.

4.5 We may, in our discretion, make Cloud Service-related scripts, schema and/or code that can be used to create process analysis applications for the Cloud Service platform (collectively, the “Celonis Schema”) available to You. In such event, You are granted for the relevant Subscription Term a limited, non-exclusive, revocable license to use and modify the Celonis Schema for purposes of implementing Your permitted use of the Cloud Service. As between You and Celonis, You will be owner of all right, title and interest in and to any modifications You make to the Celonis Schema, subject always to Our underlying ownership interest in and to all of the Celonis Schema and Services from which Your modifications derive.

5. Additional Services.

5.1 This Section applies if and to the extent We provide You with any no-cost Services (collectively, “Additional Services”). In the event of a conflict between this Section and any other portion of this Agreement, this Section shall control. In some circumstances, Additional Services are subject to limitations specified in the Order, Metrics Definition or Documentation. Your use in excess of such limits may require You to make a purchase.

5.2 Unless expressly agreed otherwise in the applicable Order, We may terminate Your access to Additional Services upon written notice at any time for any reason and without liability of any kind. Upon such termination, You will be given a reasonable opportunity to retrieve Customer Data.

5.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT (INCLUDING ANY ANNEXES OR SUPPLEMENTS HERETO) OR ANY ORDER, THE ADDITIONAL SERVICES ARE PROVIDED “AS-IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. THE SERVICE LEVEL AGREEMENT SHALL NOT APPLY TO ADDITIONAL SERVICES AND NO SUPPORT WILL BE PROVIDED. WE SHALL HAVE NO INDEMNIFICATION OBLIGATIONS OR LIABILITY OF ANY KIND WITH RESPECT TO THE ADDITIONAL SERVICES (WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT OR OTHERWISE). WHERE SUCH EXCLUSION OF LIABILITY IS PROHIBITED UNDER APPLICABLE LAW, OUR TOTAL AGGREGATE LIABILITY SHALL NOT EXCEED $1,000.00, WHICH THE PARTIES AGREE IS A FAIR AND REASONABLE AMOUNT.

6. Proprietary Rights.

6.1 As between You and Us, We are and remain exclusive owners of all right, title and interest (including without limitation the Proprietary Rights) in and to the Services. We have, and may in the course of performing the Services, develop certain general ideas, concepts, know-how, methods, techniques, processes and skills pertaining to the Services and Celonis Materials ("**Residual Knowledge**"). We shall not be prohibited or enjoined from using Residual Knowledge, other than Customer Materials and Customer Confidential Information, for any purpose, including providing services to other customers. No rights are granted to You other than as expressly set forth herein.

6.2 As between You and Us, You are and remain the exclusive owner of all right, title and interest (including without limitation the Proprietary Rights) in and to Customer Data and Customer Materials. You grant Us, Our Affiliates and any subcontractors approved a worldwide, limited-term, revocable, non-exclusive license to use, host, transmit, monitor, manage, replicate, access, collect, store, cache, analyze, aggregate and/or anonymize Customer Data, and to transfer Customer Data to Our subcontractors, in each case solely as necessary to perform the Services in accordance with the Documentation. You further grant Us and Our Affiliates a worldwide, perpetual, irrevocable, non-exclusive license to disclose key performance indicators and other information derived from Customer Data to third parties in an aggregated and/or anonymized form that will not identify You, Your Users or the Customer Data itself. No rights are granted to Us other than as expressly set forth herein.

6.3 To the extent You provide feedback regarding Our Services, products, business or development plans, or technology roadmaps, including, without limitation, comments or suggestions regarding the possible creation, modification, correction, improvement or enhancement of the Services or other products (collectively “**Feedback**”), You hereby grant Us a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate such Feedback for any legitimate business purpose without restriction. We are under no obligation to use the Feedback. Celonis acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

7. Data Protection and Customer Data.

7.1 In the performance of Our obligations to You under this Agreement, We shall maintain appropriate administrative, physical, organizational and technical safeguards for protection of the security, confidentiality and integrity of Customer

Data, including but not limited to measures designed to protect against the unauthorized access to or disclosure of Customer Data.

7.2 If in the course of providing the Services We process any Personal Data contained in the Customer Data, the Data Processing Agreement shall apply to such processing. Your use of the Services is subject to the terms of the Celonis Privacy Notice. If the terms and conditions contained at the Data Processing Agreement and the Celonis Privacy Notice conflict with State or Federal Law, the State does not agree to such terms. Further, if the terms and conditions contained at the Data Processing Agreement or the Celonis Privacy Notice conflict with the terms and conditions of Statewide 1041, the parties agree and understand that the terms and conditions of Statewide 1041 will prevail.

7.3 Each party shall, in connection with the exercise of its rights and the performance of its obligations under this Agreement, comply with all applicable Data Protection Laws.

7.4 At the conclusion of a Proof of Value, We will retain Your EMS Team, Customer Data and any analysis generated during such Proof of Value (collectively the "**POV Content**") for a maximum period of nine (9) months (the "**Dormant Period**") unless You otherwise request return or destruction of the POV Content in writing. If You purchase Cloud Services during the Dormant Period, We will reactivate Your EMS Team and transfer the POV Content to a productive EMS Team instance; if You do not, We will delete or destroy the POV Content without further notice.

8. Warranties.

8.1 We warrant that during the applicable Subscription Term: (a) the Services will substantially perform as specified in the Documentation when used in accordance with the terms of this Agreement; (b) We will not materially reduce the overall level of beneficial service provided to you under the Service Level Agreement; (c) the Services have been and will for the duration of the Subscription Term continue to be tested for Malware (including without limitation scanning with current versions of industry-standard antivirus software); and (d) Professional Services will be performed in a professional, workman-like manner with reasonable skill and care in accordance with industry standards.

8.2 Each party hereby warrants to the other that: (a) it has the authority to enter into the Agreement, to grant the rights granted by it under the Agreement, and to perform its obligations under the Agreement; and (b) it will comply with all applicable laws and regulations in effect during the term of the Agreement as they apply to such party's rights and obligations under this Agreement.

8.3

9. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

9.1 **Subscriptions**. The Initial Subscription Term of each Subscription shall be as agreed in the applicable Order. Thereafter, each Subscription may be renewed for successive periods of 12 months (each a "Renewal Term"), at the rate agreed in the applicable Order (if any), by executing a written order for the Renewal Term.

9.2 **Professional Services Term**. Each Order for Professional Services shall take effect on the Order date and remain in effect until (i) all Professional Services under such Order have been provided (and the State has accepted such Professional Services if any acceptance criteria are included in the applicable Order), or (ii) the applicable Order is terminated

9.3 **Termination for Breach**. Without prejudice to any other rights or remedies to which a party may be entitled, either party may terminate an Order without liability to the other at any time with immediate effect upon written notice if the other party is in material breach of any of its obligations under this Agreement or an Order and, in the case of a breach which is capable of remedy, fails to remedy such breach within thirty (30) days of notice of the breach. Notwithstanding the foregoing, recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the Contract Disputes Act. During any dispute under the Contract Disputes Act, Celonis shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

9.4 **Termination for Legal Cause.** We may immediately suspend performance or terminate an Order if an applicable law or an applicable government or court order prohibits Our continued performance thereunder.

9.5 **Effect of Termination.** Upon termination in accordance with this Section, and upon expiration of the Subscription Term, You shall immediately cease use of and access to the applicable Service and any Non-Celonis Application.

10. General Terms.

10.1 Publicity: The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

10.2 **Third Party Beneficiaries**. Nothing in this Agreement is intended to, nor shall create, any right enforceable by any third party not a party to this Agreement. The consent of a third party shall not be required for the amendment, variation or termination of this Agreement.

10.3 **Non-exclusive remedies.** Except where an exclusive remedy is specified in this Agreement, the exercise by either party of any remedy under the Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law, or otherwise.

10.4 Notices. All notices hereunder to US shall be in writing and shall be directed to Our Chief Legal Officer at (legal@celonis.com).

10.5 Language. Regardless of any language into which this Agreement may be translated, the official, controlling and governing version of this Agreement shall be exclusively the English language version.

Annex A Definitions

Celonis agrees and understands that any definitions, terms or condition identified in Statewide Contract No 1041 prevail over any conflicting Definitions herein, including via any embedded hyperlinks. Further, to the extent any terms and conditions within this Celonis Government End User Master Services Agreement, including via any embedded hyperlinks, violate State or Federal law, the State does not agree to any such terms.

1. "**Affiliate**": any entity that directly or indirectly controls, is controlled by, or is under common control with a party, but only for so long as such control exists. As used here, "Control," means direct or indirect ownership or control of more than 50% of the voting interests.
2. "**Agreement**": this Master Services Agreement, including (i) any Order referencing this Agreement and (ii) any terms and conditions specifically referenced in this Agreement or an Order (iii) Statewide Contract 1041.
3.
4. "**Celonis Materials**": any software, programs, tools, systems, data, Celonis Confidential Information or other materials made available by Us to You under this Agreement, excluding Non-Celonis Applications.
5. "**Celonis Privacy Notice**": the then-current privacy policy found at https://www.celonis.com/privacy-policy (current version attached hereto) and incorporated herein by reference.
6. "**Cloud Service**": the Celonis software-as-a-service platform, the On-premise Component (if applicable), and the Documentation, but excluding Non-Celonis Applications and any links to third-party products or services contained in the Cloud Service.
7. "**Customer Materials**": any materials, data, information, software, equipment or other resources owned by or licensed to You and made available to Us pursuant to facilitating Your use of the Services, including Customer Data and Output.
8. "**Data Processing Agreement**": the then-current Data Processing Agreement (including its supplements and annexes) in effect as of the effective date of Your Initial Subscription Term and each subsequent Renewal Term (as applicable) found at https://www.celonis.com/terms-and-conditions/#privacy-data-protection and incorporated herein by reference. If the terms and conditions contained at the Data Processing Agreement conflict with State or Federal Law, the State does not agree to such terms. Further, if the terms and conditions contained at the Data Progress Agreement conflict with the terms and conditions of Statewide 1041, the parties agree and understand that the terms and conditions of Statewide 1041 will prevail.
9. "**Data Protection Laws**": all applicable laws, rules, regulations, decrees, or other enactments, orders, mandates, or resolutions relating to privacy, data security, and/or data protection, and any implementing, derivative or related legislation, rule, and regulation as amended, extended, repealed and replaced, or re-enacted, as well as any applicable industry self-regulatory programs related to the collection, use, disclosure, and security of Personal Data.
10. "**Documentation**": the product description of the applicable Services, as made available by Us
11. "**EMS Team**": a password secured tenant within the multi-tenant cloud environment in which the Cloud Service runs, sharing resources across tenants and providing data isolation for each tenant.
12. "**Fees**": the fees payable by You for the Services as set out in an Order.
13. "**Initial Subscription Term**": the initial term of Your Subscription as specified in the Order.
14. "**Losses**": any and all costs, liabilities, losses, and expenses (including, but not limited to, reasonable attorneys' fees) finally awarded by a court of competent jurisdiction.
15. "**Malware**": any program or device (including any software, code or file) which is intended to prevent, impair or otherwise adversely affect the access to or operation, reliability or user experience of any computer software, hardware or network, telecommunications service, equipment or network or any other service or device, including without limitation worms, trojan horses, viruses, ransomware, trap doors and other similar malicious devices.
16. "**Metrics Definition**": the description of the Services metrics made available by Us as "Metrics Definition".
17. "**Online Training Cloud**": Online training courses offered by Celonis at https://www.celonis.com/training.
18. "**On-premise Component**": on-premise software that may be provided with, and that operates in conjunction with, the Cloud Service. When made available, the On-premise Component can be downloaded and installed (including updates) by Customer. Customer is responsible for the installation and operation of the On- premise Component, including any updates made available by Us. The Service Level Agreement does not apply to On-premise Components. If and to the extent an On-premise Component is subject to third party license terms, We will make those terms available to You with the relevant On-premise Component.
19. "**Order**": an ordering document or online order form that: (i) incorporates or references this Agreement and (ii) specifies the Services ordered and the Fees owed. Orders may be between You and Us.
20. "**Output**": means any (i) content in the form of files and/or images generated by the Cloud Service that, as part of the documented functionality of the Cloud Service, are exported, printed, downloaded and/or extracted from the Cloud Service

by an authorized User during the Subscription Term, and (ii) documentation deliverables identified as such in a statement of work for Professional Services.

21. "**Personal Data**": any data and information relating to an identified or identifiable living person as defined under applicable Data Protection Laws.
22. "**Professional Services**": the consulting and/or professional services related to the Services provided by Us to You as described in the applicable Order. Except as expressly agreed otherwise in an Order, Professional Services are limited to implementation and configuration support relating to the Cloud Service and shall in no event be considered a "works made for hire" engagement.
23. "**Proof of Value**": Your use of the Services as part of a demonstration provided by Us solely to enable You to determine whether to purchase a Subscription for the Services.
24. "**Proprietary Rights**": rights in patents, utility models, trademarks, service marks, trade names, other trade-identifying symbols and inventions, copyrights, design rights, database rights, rights in know-how, trade secrets and any other intellectual property rights, anywhere in the world, whether registered or unregistered, and including applications for the grant of any such rights.
25. "**Representatives**": of a party are its and its Affiliates' employees, officers, directors, advisers, agents and subcontractors.
26. "**Service Level Agreement**": Service Level Agreement for Celonis Cloud Service Offerings If the terms and conditions contained at the /service Level Agreement conflict with State or Federal Law, the State does not agree to such terms.
27. "**Services**": the services provided under an Order or made available to You under this Agreement, including the Cloud Service, Support Services, Additional Services, Online Training Cloud and Professional Services, each as described in the applicable Documentation. Services exclude Non-Celonis Applications.
28. "**Subscription**": the subscriptions You purchase under an Order for Your use of and access to the Services in accordance with this Agreement.
29. "**Subscription Fees**": the Fees payable for access to the Cloud Service as set out in an Order.
30. "**Subscription Term**": the Initial Subscription Term and any subsequent Renewal Terms.
31. "**Support Services**": the support services, as described in the Support Services Description, that We provide to You in respect of the Cloud Service.
32. "**Support Services Description**": the detailed description of the Support Services as included in the applicable Order.
33. "**User**": those employees, agents and independent contractors of Yours or Your Affiliates (including third-party suppliers and/or contractors) who are authorized by You to access and use the Services in accordance with this Agreement, and to whom You have supplied a user identification and password (if applicable).
34. "**We**," "**Us**", "**Our**" or "**Celonis**": the Celonis entity entering into the applicable Order with You or fulfilling the applicable Order placed with an Authorized Reseller.
35. "**You**" or "**Your**": the instrumentality of the U.S. Government conducting ordering activity under GSA Schedule Contracts that enters into the applicable Order.

celonis

ATTACHMENT E-4 to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199

The Celonis Support Services is hereby amended to include the terms as set forth below and supersedes all prior Celonis Support Services submitted by Celonis or discussed by the parties.

Celonis Support Services

Celonis has implemented a set of Support Services to make sure You experience a high level of service. We will be happy to provide the following Support Services to You as part of Your purchase or subscription of the Celonis Software. You can contact the Celonis Support team via a broad set of channels, according to Your specific needs and whichever best suits Your inquiry.

1 Releases (Maintenance)

As part of the Celonis Support Services, You will receive, at no additional charge, all generally available releases of the Celonis Software which You have licensed. Releases may address security fixes, critical patches, general maintenance functionality, and documentation.

1.1 Cloud Services

As You are a subscriber to the Celonis SaaS offering, we will upload the release automatically, so You do not have to worry about this. The Support Services will then be rendered to the updated software version only.

We may enhance the features of our Cloud offering, for example to reflect technical advances or to comply with laws; however, we are under no obligation to develop any future functionality, programs, services, or enhancements. If we do make updates or enhancements, we will notify You about them and the date they are to take effect by email, through the Celonis Service Desk Portal, Release Notes or within the Cloud offering.

If You have any queries relating to on any of such updates or enhancements, please contact our Support Services team using the Celonis Customer Support Portal.

1.2 On Premise Edition

You can download each respective release from the *my.celonis* portal. However, the service of downloading and installing the release to Your On-Premise server is not included in the Support Services.

1.3 Security Updates

Whenever we provide a release, a patch, or a fix with relevance to Security Incidents or other security-related issues, we offer to notify You via email. In order to receive such emails, You are required to provide us with the contact details (email address and telephone number) of the contact person best suited for this matter. To provide the contact details You can send an email with the information to the following email address:

security-incident@celonis.com

APPROVED celonis BY LEGAL

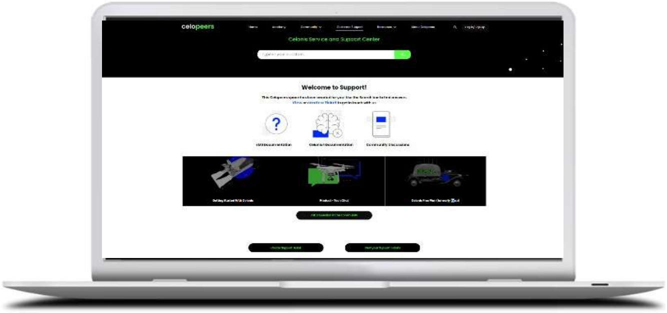
1.4 Usage Information

In order to provide You with improved transparency on the utilization of Your Cloud Service, we may collect and analyze information derived from your use of the Cloud Service (e.g. how many processes are used, which online trainings were performed). Neither information related to individual users nor any Customer Data is used for these purposes.

2 Service Desk, Global Phone and Email Support

As part of the Celonis Support Services, You will benefit from free access to the Celonis Service Desk Portal. This is often the most efficient way to get answers to common questions as it allows you to submit and track support requests.

https://www.celopeers.com/s/



Celonis Support Services include a highly trained team of Celonis experts located in our Celonis Support Centers. Our system engineers are familiar with the common challenges organizations face when deploying Celonis software and can quickly diagnose and support questions regarding product-related issues you are facing.

2.1 Overview Global Phone and Email Support

	EMEA	AMERICAS
SERVICE TIMES	Mon – Fri Business hours only 9 am – 5 pm (CET)	Mon – Fri Business hours only 9 am (EST) – 8 pm (EST)
LANGUAGES	English, German	English
PHONE	+ 49 (0) 89 4161596 – 77	+ 1 917 – 830 - 6806
EMAIL	servicedesk@celonis.com	servicedesk@celonis.com

If You are located outside of EMEA and the Americas, please refer to whichever support center best suits your business hours.

2.2 Premium Support

Celonis Premium Support is available only for Celonis EMS and includes unlimited phone and email access to the support team on a twenty-four hour, seven days a week basis. You can elect Celonis Premium Support for an additional fee. For more information, please contact your Celonis sales representative.

3 Manual & Training Material

In addition, You will have free access to the my.celonis portal. The my.celonis portal provides a comprehensive knowledge base containing answers to many common product questions and a manual that covers common product topics. Here, You will find training material covering the basics of how to work with the Celonis software.

The Celonis Academy provides extensive training courses, starting from the very basics and extending to expert level mastery of the Celonis technology. Please refer to your Celonis sales representative for more information.

4 Incident Reporting and Response Times

4.1 Ticket Reporting

When raising a Support Inquiry via the Celonis Portal at www.celopeers.com, You have the opportunity to select the Type of your Support Inquiry, as further defined in 4.2 below.

When requesting Celonis Customer Support Services via email, we will open a Support Ticket for You and determine – to the best of our knowledge – the Type and Severity. We will then notify You of the created ticket number, which enables the accurate placement of subsequent queries within the Support Ticket Management System.

4.2 Ticket Types

TICKET TYPE	DEFINITION
INCIDENT	An Incident is affecting Your ability to use the Celonis Software. Something, which worked in the past, is not working as expected and resolution is required from Celonis for this. Additionally, only for this type of Incident, the severity can be selected based on the criteria described in 4.3.
SERVICE REQUEST	A request for a Service from Celonis. For instance, to have some feature or function of the Celonis Software enabled for You; or You require help with access rights for a specific person or a specific area is needed.
QUESTION	A technical Question on how a specific Celonis Software feature, function, or product works. Or You require help with a specific code snippet or insights on how the code is working.
FEATURE REQUEST	Suggestion for a new feature or enhancement of an existing feature of the Celonis Software. However, we are under no obligation to develop any future functionality, programs, services, or enhancements.

4.3 Incident Severity definitions

If You selected the Type of Your Support Inquiry as an Incident, following Incident Severity Types can be assigned to your Inquiry.

INCIDENT SEVERITY	DEFINITION	EXAMPLES
1, CRITICAL	Use of the Celonis Software is not possible or practically not possible due to the impairment and your business is totally affected.	● Single Service (e.g. Data Integration, Action Engine, Machine Learning) is unreachable ● The entire realm is unreachable ● DNS not resolving

2. SEVERE	Work with the Celonis Software is seriously affected, and necessary business tasks cannot be performed.	● Increased latency (long load times, timeouts)

		● Increased error rate (request intermittently fail) ● Data Model cannot be queried ● Data Jobs not executing ● ML Apps not starting/opening
3, MEDIUM	A feature or function of the Celonis Software is affected, and does not perform as desired, with medium business impact.	● DB jobs not executed in the first time ● Pods of new deployments in
4, MINOR	A feature of function of the Celonis Software is affected, and does not perform as desired, with minor business impact.	● Issues around usability and layout

Celonis Customer Support will review the Severity of each Incident and will make reasonable adjustments to the Severity Type in line with the above definitions, where the originally selected Severity Type does not align with the table above.

4.4 Incident Severity Definitions

After the assignment of a ticket number and a Severity (in accordance with table 4.2), we will use commercially reasonable efforts to respond to the Incident within the Target Initial Response Times (see below). The Initial Response Time shall be measured by the time between a complete ticket being correctly submitted and the time we acknowledge receipt of the ticket. You understand and agree that full resolution of an issue is not guaranteed and that the actual time required to resolve any issue may be longer than the Initial Response Time.

SEVERITY	DEFINITION
SEVERITY 1, CRITICAL	2 hours
SEVERITY 2, SEVERE	24 hours
SEVERITY 3, MEDIUM	48 hours
SEVERITY 4, MINOR	96 hours

The Response Times are calculated during the local service times. If during the course of the support process the Incident no longer warrants the currently assigned severity, we may change the priority of an Incident to best reflect its actual severity.

We may consider an Incident as dropped and subsequently close the Incident if You have not responded within five business days to our attempt to collect additional information required to resolve the incident.

Whenever we determine an Incident is not due to any error or deficiency in the Celonis Software we will have no obligation to provide any Celonis Support Services regarding the Incident (For example, such incidents may be caused, without limitation, by issues or problems caused by the internet or other communications, or your network or browser matters, or login issues).

5 Changes to the Support Services Description

During the subscription term, we will have the right to update this support services description in accordance with the applicable Terms & Conditions of Your Celonis product.

celonis

ATTACHMENT E-5 to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199

This document is hereby amended to include the terms as set forth below and supersedes all prior versions submitted by Celonis or discussed by the parties. The terms and conditions of SW1041 prevail over any conflicting terms and conditions in this document.

Definition Subscription Scope:

Execution Management System

This document specifies and defines the metrics referenced within the subscription scope of each individual Order entered into between You and Us. The provisions of each individual Order prevail over the below definitions in the event of and to the extent of a conflict.

Analytical Processing Capacity (APC)

The APC is the amount of uncompressed raw data that the customer ingests into the Execution Management System (EMS) concurrently at any given time for processing. The processing of data within EMS includes transformations, high-performance computation and storage. APC is priced at standard level (aligned with Productive EMS Team) and premium level (aligned with Premium-Productive EMS Team).

EMS Team

An EMS Team is a password-secured tenant within the multi-tenant cloud environment in which the Cloud Service runs, sharing resources across tenants and providing data isolation for each tenant. When provisioning the EMS Team, we will select the most applicable multi-tenant cloud environment for You.

1.1 Productive EMS Team

The Productive EMS Team is provided as a part of Business User, Analyst and APC subscriptions according to the respective Order and includes components (e.g. Transformation Center, Process Automation) according to the applicable Product Description. The scope of Business Users, Analysts and APC is limited to the purchased number in the respective Order.

On the Subscription Start Date, the Admin User will receive an invitation email with initial log-in details to access the Productive EMS Team. Access is for the Subscription Term only.

1.2 Standard Sandbox Team

The Standard Sandbox Team serves as a testing environment for independent evaluations and testing within the limits of the defined table rows. The Standard Sandbox Team is provisioned per default upon the rollout of Your Productive EMS Team. Your Standard Sandbox Team cannot be connected to any other system that is not itself a Sandbox/testing environment. The following scope is included in Your Standard Sandbox Teams: the number of Analysts is limited to the number specified in the respective Order for your Productive EMS Team and You'll receive 10% of the APC in relation to the purchased amount of APC in Your Productive EMS Team Table rows are limited to 100,000 rows and no Business Users are provided.

1.3 Premium Sandbox Team

The Premium Sandbox Team serves as a testing environment for independent evaluations and testing within the limits of the defined table rows. The Premium Sandbox Team is only available as a separate Order at an extra charge and will not be provisioned per default. Your Premium Sandbox Team cannot be connected to any other system that is not itself a Sandbox/testing environment. The following scope is included in Your Premium Sandbox Team: the number of Analysts is limited to the number specified in the respective Order for Your Productive EMS Team and You will receive the same amount of APC as supplied for Your Productive EMS Team. There are no limitations regarding Table Rows. No Business Users are provided in Premium Sandbox Team.

1.4 Premium Productive EMS Team

The Premium-Productive EMS Team includes all of the feature of the Productive EMS Team while also providing for an unlimited number of users, each a single natural person designated by name, all of whom may:

- view and interact with analyses built and shared in the Execution Management System;
- build and edit data models, machine learning models, skills and analyses in the Execution Management System;
- utilize full administrative capabilities; and
- create, receive and interact with Executions from the Action Flow and take respective actions on such signals.

The Premium-Productive EMS Team also includes access to the Celonis EMS Connector for Power BI and the Intelligence API.

Business User

1.1 Definition

A "Business User" describes a personalized password protected account for access to the respective Celonis product specified in the individual Order. A Business User is limited to accessing and filtering analyses built and shared in the Execution Management System. In addition, the Business User can receive and interact with Executions from the Action Flow and take respective actions based on such signals.

1.2 Scope

A Business User may only be used by one single natural person designated by name. A Business User may not be made accessible to any third person, including employees of the same company or of affiliated companies. You are entitled to replace the person associated with the Business User by way of updating the name so-designated in the system. The number of subscribed Business Users constitutes an upper limit for the number of employees authorized to access the Execution Management System.

Analyst

1.1 Definition

An "Analyst" describes a personalized password protected account for access to the respective Celonis product specified in the individual Order. This access includes all subscribed features, only limited by the elected individual user rights, whereas the individual user rights may be elected and altered freely. Therefore, the User has full flexibility and in addition to viewing and interacting, the User can also build and edit data models, machine learning models, skills and analyses in the Execution Management System. Additionally, the User has full administrative capabilities and can create, receive and interact with Executions from the Action Flow and take respective actions on such signals.

1.2 Scope

An Analyst may only be used by one single natural person designated by name. An Analyst may not be made accessible to any third person, including employees of the same company or of affiliated companies. You are entitled to replace the person associated with the Analyst by way of updating the by name so-designated in the system. The number of subscribed Analysts constitutes an upper limit for the number of employees authorized to access the Celonis Software.

Executions

Executions are Actions (automated events) that take place in the Operational System of a customer as a result of running an Action Flow. An Execution occurs every time a record is created, updated or deleted in an Operational System (transactional systems such as CRM, HRM or ERP as well as databases and other specialized source systems).

Each EMS Subscription includes a capacity of 150,000 Executions per contract year (i.e. each 12-month period initially measured from the commencement date of the Subscription, and measured from each anniversary thereof). Exceeding this capacity will result in a requirement to subscribe to additional capacity (Executions) in accordance with the agreed pricing or the then-current list price will be applied. The additional capacity will be reflected in an additional Order.

Customers can subscribe additionally to a specified number of Executions upfront to ensure sufficient capacity of Executions per contract year which will be also reflected in an Order. The subscribed amount of Executions constitutes an upper limit for the number of Executions that can be performed within the Celonis Action Flows per contract year. Executions not used within one contract year will not roll over to the next contract year.

Workbenches

Each EMS Subscription includes the Machine Learning feature which consists of 3 Workbenches. Per Workbench, 4 GM RAM (Random-Access Memory), 1 CPU (Central Processing Unit) and 5 GB Disk Space are included per default. Additionally, the Auto-Shutdown function is enabled which will shut down each Workbench after 12 hours of non-usage. The Auto-Shutdown does not apply to scheduled runs. For heavy Machine Learning workloads, a dedicated instance is available as an add-on product which will be reflected in an individual Order.

Annual Open Invoices

The subscription scope of the Accounts Receivable Business App is based on Annual Open Invoices. An Annual Open Invoice means an individual newly-created invoice that has been extracted from Your source system and processed within the Accounts Receivable Business App. The subscribed volume of the Annual Open Invoices is defined in the applicable Order. It denotes the number of Annual Open Invoices in scope for each contractual year of the subscription.

Process Sphere is an incremental add-on to EMS Standard and Premium and is priced based on Object Types and Transaction Value:

Object Types

An Object Type is a defined item in the data model that reflects a group of multiple instances of the same object that is of interest. For example, while an individual Sales Order, Sales Order Item, Delivery, Invoice, or Invoice Item would be considered an “object,” the group consisting of all Sales Order objects would be an Object Type. One process can have multiple Object Types and each Object Type can be reused across multiple explorations within a single process, or potentially across multiple processes, within Process Sphere.

The total number of all unique Object Types across the customer´s Process Sphere explorations cannot be more than the subscribed amount specified in the applicable Order.

Transaction Value

Transaction Value is the sum of the values of all objects within a process' Main Object Type that are processed within Process Sphere. All processes have one "Main" Object Type that is used to calculate the Transaction Value. Here is a list of the Main Object Types used for common process types:

- Order Management: Sales Order Header
- Accounts Receivables: Customer Invoice Header
- Procurement: Purchase Order Header
- Accounts Payable: Vendor Invoice Header
- Claims Management: Claims Total Value
- Inventory Management: Inventory Total Value

An object within the Main Object Type is deemed processed the first time it is loaded into Process Sphere. Upon processing, each object´s USD value is consumed from the purchased Transaction Value.

The subscribed Transaction Value is expressed in US Dollars within the applicable Order, and denotes the total amount of Transaction Value that can be processed within each year of the Subscription. All values are converted at the average FX rate for the day the respective object within the Main Object Type is processed. Transaction Value not used within one subscription year will not roll over to the next subscription year. If the customer consumes all of its contracted Transaction Value, the customer may not be allowed to process new Objects into Process Sphere until the customer purchases additional Transaction Value.

If the process being explored in Process Sphere is among those listed above but doesn't have the specified Main Object Type, then Celonis will use the closest logical Object Type to assess the Transaction Value. For example, if the Customer does not have a Customer Invoice Header, the next logical Main Object Type to work with is an Invoice Item Line, and so on.

If the process being explored in Process Sphere is not among those listed above, then the Main Object Type used to calculate the Transaction Value will be as specified in the applicable Order Form.

Workforce Productivity is an incremental add-on to EMS Standard and Premium, priced based on Active Concurrent Users:

Active Concurrent User

An Active Concurrent User is a unique user, represented by the combination of a username ID and a unique machine ID, sending or capturing data at any given time during a calendar month of the subject EMS subscription.

The amount of permitted Active Concurrent Users is specified in the applicable Customer Order. Customer is permitted to reassign Active Concurrent Users amongst its employees, provided the number of assigned Active Concurrent Users at any given time does not exceed the limit specified in the applicable Order.

The Subscription Scope for the Celonis Execution Management System as described herein replaces the defined Subscription Scope for the Celonis Intelligent Business Cloud as of its release date. Therefore, all features previously described in the documents relating to the Celonis Intelligent Business Cloud are now collectively described in this Metric Definition for the Celonis Execution Management System and its successive versions. Please note that the preceding provisions do <u>not</u> apply to licensees of SAP Process Mining by Celonis, Cloud Edition.

**ATTACHMENT E-6 to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199**

This document is hereby amended to include the terms as set forth below and supersedes all prior versions submitted by Celonis or discussed by the parties. The terms and conditions of SW1041 prevail over any conflicting terms and conditions in this document.

PRODUCT DESCRIPTION:

Execution Management System

The Celonis Execution Management System (EMS) is a technology built to achieve execution capacity breakthroughs. The EMS consists of real-time data connectivity, the Core Mining Engine, the Automation Engine, the Celonis Studio and the EMS Marketplace that all run on the EMS platform.

1. Real-Time Data & Platform

FEATURE	DESCRIPTION
INTELLIGENCE API	
CELONIS EMS CONNECTOR FOR POWER BI	The Celonis EMS Connector for Power BI is an addition to Power BI that allows You to natively connect Power BI to Your Celonis EMS instance as You would connect, for example, to a SQL-based database. The Celonis EMS Connector for Power BI will automatically list all published knowledge models and allow the importing of records that are defined in the knowledge models. You will be able to define records in PQL inside the knowledge models and load them not Power BI, enabling the full PQL experience inside Power BI. The Celonis EMS Connector for Power BI is limited to a maximum of 200.000 rows and 20 columns and is only available within the Premium EMS Team.
DATA LAKE	s that will create the Event Logs.
DATA INTEGRATION	Data Integration connects to a multitude of source systems to capture events in th form of digital footprints. Furthermore, it allows the User to transform the extracted

	data to construct a data model. The data pipeline can be orchestrated and automated through an user interface.
PROCESS CONNECTOR	The Process Connector is the combination of extracting, connecting and transforming data for one source system. **System Extractor** The System Extractor is the software component that extracts data from the source system and sends it out to EMS. **Data Job** A Data Job is the collection of data integration tasks which extracts and transforms the source system data and makes them available in the EMS. **Data Model** The Data Model is the logical description on how events and other data are related to each other. This can include one or multiple Event Logs.

2. Core Mining Engine

The Core Mining Engine is an in-memory engine that leverages process mining to measure execution capacity and identifies execution gaps. It works with business logic or Machine Learning to sense gaps that have the biggest impact on execution capacity and trigger actions in the Automation Engine.

FEATURE	DESCRIPTION
CELONIS PQL	
MACHINE LEARNING	Machine Learning (1) provides other Celonis Products such as Process Analytics, Action Flows, or open application framework applications with advanced analytics data including predictions, simulation scenarios, or analysis of unstructured data, (2) is a platform for data scientists to build advanced analytics use-cases in an open ecosystem, (3) contains a python package to help the User solve the most common process related Machine Learning tasks. For heavy Machine Learning workloads, a dedicated instance is available as an add-on product.
MULTI-EVENT LOG	-joins when defining activities. Users can identify inefficiencies using cross-process KPIs and visualize end-to-end processes within a single analysis.

SIGNAL LINK	The Signal Link defines an out signal to link the data to each other written in the transformation script.

3. Automation Engine

Action Flows provide a real-time automation engine integrated with Celonis' process mining technology to perform next-best actions in cloud, on-prem, and custom applications. Next-best actions comprise unattended automations in enterprise IT systems as well as "human in the loop"-type automations by creating tasks & alerts for users in the EMS. Action Flows can be built using a no code drag & drop builder.

FEATURE	DESCRIPTION
DRAG & DROP ACTION FLOW BUILDER	
PRE-BUILT AUTOMATIONS	Use 10,000+ pre-built automations across 700+ applications to perform automations.
ON-PREM AUTOMATIONS	Automate in 15+ enterprise on-prem applications using the Celonis On-Prem Agent.
AUTOMATIONS IN CUSTOM SYSTEMS	Perform API-based automations in custom systems.
PROCESS MINING INTEGRATION	
ADVANCED ERROR HANDLING	Use advanced error handling features to recognize and resolve issues before they become apparent to the business.
ADVANCED AUTOMATION TOOLING	
SCHEDULED ACTIONS	Schedule whenever an Action Flow should be executed (e.g. daily, every Tuesday at 9 am, ...).

4. Celonis Studio

The Celonis Studio is a low code development interface that allows the User to build, customize, package, and publish execution applications and process analyses. The Celonis Studio is made up of a few key building blocks: Skills, Views, Analysis, and folders.

FEATURE	DESCRIPTION
ALERTS & RECOMMENDATIONS	
PACKAGES	Packages are the main structural element in the Celonis Studio and contain collections of assets that interact with each other to generate an execution app. Within packages the User can create Views, Skills, Knowledge Models and Analysis.
SKILLS	re Action Steps that define what happens after the Sensor is triggered. Skills are executed by the Celonis Automation Engine. The Action Steps can be automations (API calls) to other systems, alerts to end-users, or prioritization of work in Celonis user-specific Views.

a. Analyses Features in the Celonis Studio

FEATURE	DESCRIPTION
ACTIVITY EXPLORER	
BOOKMARKS	Bookmarks can be used to store findings. By setting a bookmark, the currently used filters will be saved for future use.
CASE EXPLORER	
CHARTS AND TABLES	Charts and Tables can be created and edited to illustrate certain data. The following components can be used: OLAP tables, column charts, pie charts, donut charts, line charts, area charts, marker charts, scatter plots, bubble plots, histogram charts, single KPIs (gauge, number, fill, and radial), pivot tables, box plots, and world maps.
CONFORMANCE CHECKER	The Conformance Checker uses artificial intelligence to automatically detect non-conformant cases and to outline their violations, root-causes and impact on KPIs, by comparing the mined as-is process against a target process model. To define the target model, the Conformance Checker supports importing .bpmn files (BPMN 2.0 Standard), modeling processes with the built-in process modeler or automatically documenting the mined as-is process as the target model.

DESIGN COMPONENTS With Design Components the User can enrich the analysis sheets with various design features. The following components are available: variable input, button, button dropdown, text components, image, line, logo.

FILTERING Dynamic filters allow the User to create selections from any component of an analysis sheet, filtering the whole analysis document. Only cases that meet the selected filter criteria are then examined in the components.

KPI LIBRARY Saved formulas allow the User to create their own reusable KPI Library. It is possible to define replaceable parts of the formula with the help of customizable parameters. Thereby the User can define which parts of the formula are editable by other users.

PROCESS EXPLORER The Process Explorer allows the User to explore the process based on the frequency of activities performed in the process.

PROCESS REPOSITORY The Celonis Process Repository is an integrated and centralized environment for documenting and maintaining business processes. It supports versioning and it integrates with third party Business Process Management tools. The stored models can also be accessed directly from the Conformance Checker.

PROCESS SIMULATION Process Simulation allows the User to measure the impact of possible changes on Your processes and their effect on Your operations. You can dynamically simulate all parts of the process and, thereby, assess optimizations without risk.

SELECTION COMPONENTS Selection Components are built to facilitate the creation of filters. The following components can be used: dropdown, date picker, cropping, search.

SELECTION VIEWS Selection Views are predefined filters, which enable the User to filter based on a selection of attributes, activities, process flows, throughput times, rework rates, or cropped subprocesses.

THROUGHPUT TIME SEARCH The Throughput Time Search allows the User to examine the throughput time between two specific activities.

VARIANT EXPLORER The Variant Explorer allows the User to explore the process based on the end to end variants.

5. EMS Marketplace

The Marketplace allows for distribution and no-code installation of execution apps and instruments developed in the Celonis Studio. You can use it to distribute applications and instruments publicly on a market place that allows them to be sold. As a customer you will find execution apps and instruments ready for installation for various processes and use cases.

a. Execution Applications

Celonis Execution Apps are intended to identify execution gaps and deliver an approach to fix them. They are tailor-made for specific processes with pre-built, role-based views, best practice KPIs, and Action Flows.

Celonis provides two types of Execution Apps:
i) Standard Execution Apps, which facilitate the quick discovery of value within your processes. Celonis Standard Execution Apps are available at no cost for self-installation within the Marketplace; and
ii) Premium Execution Apps, which go beyond the initial "identify and fix" and leverage best-practice process knowledge to resolve root causes quickly. They are compact and targeted pre-built solutions that deliver:

1. Advanced functionalities for complex use cases (e.g. Shipping emission opp);
2. Combined insights from multiple processes (e.g. Inventory opp); or
3. An operational workspace within which a process can be executed, monitored and managed on an ongoing basis (e.g. AR apps).

Premium Execution Apps are separately purchasable as additional modules alongside the standard EMS functionality.

i. Standard Execution Apps

Celonis provides Quickstarts for Accounts Payable, Accounts Receivable, Inventory Management and Order Management. The apps help customers to identify, prioritize, and resolve process inefficiencies fast, minimizing the time-to-value and maximizing the value of Celonis for our customers.

ii. Premium Execution Apps

Celonis AR Apps

The Celonis AR Apps consist of three use-case specific applications for Collections, Credit and Disputes. The apps provide a 360-degree view of AR operations by connecting data across all source systems, apps and desktops.

They enable data-driven prioritization and risk assessment by taking into account various influencing factors and past behavior. They then enable role-based, intelligent execution by identifying common inefficiencies and triggering appropriate actions in real-time.

Sustainable Spend Management App

The Sustainable Spend Management App unifies siloed Procurement & ESG (Environmental, Social & Governance) data sources including purchase requests, ESG scorecards and high-risk suppliers into a single solution to boost the productivity of Category Managers by helping them to meet the highest ESG standards expected by customers, regulators and investors.

The App offers a single solution to view, prioritize and efficiently manage supplier sustainability. It integrates sustainability ratings and scorecards of suppliers into the Celonis EMS, integrates high-risk suppliers indicated by a rating provider, recommends which suppliers to prioritize and streamlines taking action to request ESG rating.

6. Process Analyses

Process Analyses enable analysts to measure execution capacity and identify execution gaps. They are tailor made to measure specific KPIs on a unique process and contain pre-built views for analysts.

7. Other Components

Transformation Center

The Transformation Center helps the User monitor the performance of all Your processes in one central place. It provides the User with an overview of Your objectives and KPI development. The Transformation Center is designed to measure the success of Your process improvement and transformation initiatives.

In the Transformation Center, the User can define qualitative objectives (e.g. strategic initiatives) and assign associated quantifiable KPIs for any data model. This allows You to align Your team, department and company and monitor your transformation journey.

Platform & Team Management

The platform administration is a set of capabilities and administrative controls that correspond to all aspects of the EMS platform, including deployment settings & configuration, licensing and team management.

FEATURE	DESCRIPTION
APPLICATION KEYS	Application Keys are used to authenticate scripts and applications.
PERMISSION & ACCESS CONTROLS	With the Permission & Access Control You are able to authorize different Data and User Permissions in the EMS Team.
TEAM SECURITY & PRIVACY	-ins will be tracked additionally.
USER AUTHENTICATION	User Authentication tells the system who the User is and authenticates the business system underneath. It also contains Celonis Identity Provider, which enables management of user accounts within the EMS Team and a Single Sign On function that integrates the EMS with user authentications via active directory or similar in order to require all users to login with a central user account.
USER MANAGEMENT	t of Users, Analysts and Admins and the Team can be organized into specific User Groups.

8. Optional Components

The following optional components are available at an additional cost to Standard and Premium EMS customers.

COMPONENT	DESCRIPTION
WORKFORCE PRODUCTIVITY	The Celonis Workforce Productivity component enables businesses to securely collect and analyze user interactions on desktops in order to increase efficiency by gaining full visibility, understanding changing behaviors and capturing employee experience. In order to be in line with individual requirements, this component is highly configurable and data capturing can be limited according to each specific use case. The law varies significantly between countries and use-cases, therefore You are advised to consult Your legal experts before activating Workforce Productivity for Your Users. Celonis bears no liability for Your use of this functionality.

BUSINESS MINER

Tailored to users who are experts in their business processes but less familiar with EMS, Business Miner is a quick and easy way of looking into different aspects of business processes. With Business Miner, You can leverage the powerful functionality of EMS without having to understand all of its technical details. By selecting and answering a series of simple questions, it is possible to retrieve detailed information about your business processes, get suggestions on how to improve them, discover potential savings by optimizing Your processes and collaborate with Your colleagues in a shared space. Moreover, a simplified onboarding experience enables new users to quickly get started. Business Miner makes the power of Celonis EMS accessible to a new, non-technical audience across the enterprise in order to significantly increase and accelerate business performance.

PROCESS SPHERE

Process Sphere delivers a completely new experience for users to explore their end-to-end processes in a powerful, intuitive, and consumable way. This solution broadens the perspective of process mining from analyzing a process through a single case ID to analyzing the entire business through the real-world relationships between objects and events. Objects are the individual items that are processed, for example, invoices, sales orders or purchase orders. Events are the process steps relating to those objects such as approvals, changes, or status updates. Process Sphere brings a complete and accurate 3-dimensional view of end-to-end business process execution as it occurs in reality and for the first time, customers can visualize their end-to-end processes in one interactive exploration.

The Celonis Execution Management System is a cloud service accessed via web interface. Full functionalities are only available in a full cloud deployment.

This Product Description for the Celonis Execution Management System replaces the Product Description for the Celonis Intelligent Business Cloud as of its release date. Therefore, all features previously described in the documents relating to the Celonis Intelligent Business Cloud are now collectively described in this Product Description for the Celonis Execution Management

System and its successive versions. Please note that the preceding provisions do <u>not</u> apply to licensees of SAP Process Mining by Celonis, Cloud Edition.

ATTACHMENT F to
STATE OF OKLAHOMA CONTRACT WITH
Celonis, Inc.
RESULTING FROM SOLICITATION NO. 0000000199

The Contract is hereby amended to include the terms as set forth below and supersedes all prior terms and exceptions submitted by Celonis, Inc. or discussed by the parties.

Requested Exceptions and Additional Terms not addressed below are declined by the State of Oklahoma.

Section	Exception/Notes
Attachment B, Section 11	Any reference to "immediately" in Section 11 (Confidentiality) of Attachment B to the Contract shall be replaced with the term "without undue delay".
Attachment B, Section 11.1	Section 11.1 of Attachment B to the Contract is hereby modified to add the following language to the end of Section 11.1: "Each party retains all Intellectual Property Rights in its Confidential Information. For sake of clarity, each party may disclose Confidential Information for purposes of performing under the Contract and who agree, in writing, to keep the information confidential on terms no less restrictive than those contained in the Contract."
Attachment B, Section 13	In addition to the assignment rights set forth under Section 13 (Assignment and Permitted Subcontractors) of Attachment B to the Contract, each party may delegate such party's performance under the Agreement to its Affiliates. No performance obligations under this Contract may otherwise be assigned without prior notice and written approval and consent by the State except as otherwise set forth under the Cover Page to the Contract or Attachment F-Exceptions. Any assignment of performance obligations does not relieve Supplier of their obligations under the Contract.
Attachment B, Section 13.3	The last sentence in Section 13.3 of Attachment B to the Contract is hereby deleted in its entirety and replaced with the following new language: The State may object to the appointment or replacement of a Supplier subprocessor prior to its appointment or

	replacement, provided such objection is in writing and based on reasonable grounds as follows: (a) such subprocessor would be in violation of the terms of the Contract if so appointed; (b) such subprocessor would pose a material risk to the security of the State's Customer Data if so appointed; or (c) other reasons relating to the protection of Customer Data intended to be processed by such subprocessor if so appointed. Moreover, the State reserves the right to request the removal of, and Supplier agrees to promptly remove, any of Supplier's subcontractors (or employees thereof) performing Professional Services under the Contract in the event of: (i) any act or omission on the part of such subcontractor which amounts to serious intentional or willful misconduct, or (ii) demonstrable improper conduct or lack of qualification of a subcontractor to perform Supplier's obligations.
Attachment B, Section 16.1	Section 16.1 A. (Acts or Omissions) of Attachment B to the Contract is hereby modified by adding the term "real or tangible" before property in subsections A and B of Section 16.1). Section 16.1 if further modified by adding a new subsection C to Section 16.1 as follows: "C. Notwithstanding anything to the contrary in Section 16.1 A., subject to the Supercap set forth in Section 16.5 E of this Attachment B, Supplier shall indemnify, defend and/or settle at Supplier's expense and hold the Indemnified Parties harmless from any (i) third party claims, suits, actions, injunctions, damages, losses, liabilities (in each case, as awarded by a court of competent jurisdiction), (ii) any settlement amount approved by and agreed to in writing by the indemnifying party, and (iii) actual costs or expenses (including reasonable attorneys' fees) that the Indemnified Parties may incur, and in each case, arising out of or related to any action or claim brought against the Indemnified Parties by a third-party as a result of a confirmed Data Breach or Security Incident involving or impacting Customer Data (collectively, a "Data Security Incident Indemnity") caused as a result of Supplier's breach of Supplier's obligations under the Contract."

Attachment B, Section 16.2	Section 16.2 (Infringement) of Attachment B to the Contract is hereby amended be deleting the following from the first sentence in Section 16.2: "Supplier's breach of its representations and warranties in the Contract or" Section 16.2 (Infringement) of Attachment B to the Contract is further amended by adding the following as a new paragraph to the end of Section 16.2: "For sake of clarity, Supplier's sole indemnity obligation under Section 16.2 shall be with respect to any third-party infringement claim alleging infringement of any patent, intellectual property, copyright or other proprietary right in connection with Services (as the term is defined in Attachment E-3) or Customer's use of the Services (or any part thereof) in compliance with the Contract (each an "Infringement Claim")."
Attachment B, Section 16.2	Section 16.2 (Infringement) of Attachment B of the Contract is hereby modified by adding the following paragraph to the end of Section 16.2: "In the event of an Infringement Claim, and in addition to Supplier's indemnity obligations, including Supplier's Infringement Indemnification obligations under 16.5 B, Supplier, at their option and expense: (i) modify or replace the affected Service to eliminate the alleged infringement without loss of material functionality; (ii) procure a license to enable Customer to continue using the Services; or (iii) terminate Customer's Order for the affected Services with immediate effect and refund any prepaid Fees covering the remainder of the applicable Subscription Term."
Attachment B, Section 16.3	Section 16.3 (Notice and Cooperation) of Attachment B to the Contract is hereby modified by adding the following to the end of the last sentence in Section 16.3: "or in the case of an Infringement Claim, cessation of use of the allegedly infringing product."
Attachment B, Section 16.5	Section 16.5(A) is deleted in its entirety and replaced with the following: With respect to any claim or cause of action arising under or related to the Contract, neither party or any affiliate shall be liable to the other for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

Attachment B, Section 16.5	Subsection B of Section 16.5 (Limitation of Liability of Attachment B to the Contract is deleted in its entirety and replaced with the following new subsection B: "TO THE EXTENT PERMITTED BY LAW, NO PROVISION, INCLUDING THOSE IN SECTION D GENERAL LIMITATION, SHALL LIMIT DAMAGES, EXPENSES, COSTS, ACTIONS, CLAIMS AND LIABILITIES ARISING FROM OR RELATED TO: (A) SUPPLIER'S INFRINGEMENT INDEMNIFICATION OBLIGATION, (B) EITHER PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY A PARTY'S NEGLIGENCE OR THAT OF ITS REPRESENTATIVES, (C) EITHER PARTY'S FRAUD OR FRAUDULENT MISREPRESENTATION, (D) EITHER PARTY'S WILLFUL MISCONDUCT OR GROSS NEGLIGENCE, (E) EITHER PARTY'S VIOLATION OF THE OTHER PARTY'S PROPRIETARY RIGHTS, (F) EITHER PARTY'S PAYMENT OR REFUND OBLIGATIONS UNDER THIS AGREEMENT (AS APPLICABLE), OR (G) EITHER PARTY'S LIABILITY WHICH CANNOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW."
Attachment B, Section 16.5	Section 16.5 of Attachment B to the Contract is hereby modified by adding the following new subsection D to the end of Section 16.5: "D. GENERAL LIMITATION. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE CONTRACT, IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY AND ITS AFFILIATES AND SUPPLIERS ARISING OUT OF OR RELATED TO THIS CONTRACT EXCEED THE GREATER OF: (A) THE TOTAL AMOUNT OF FEES PAYABLE BY YOU FOR THE SERVICES GIVING RISE TO THE LIABILITY IN THE TWELVE MONTHS PRECEDING THE DATE OF THE EVENT FOR WHICH THE LIABILITY ARISES; OR (B) ONE MILLION DOLLARS ($1,000,000 USD). THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) AND REGARDLESS OF THE THEORY OF LIABILITY."
Attachment B, Section 16.5	Section 16.5 of Attachment B to the Contract is hereby modified by adding the following new subsection E to the end of Section 16.5: "SUPERCAP. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE CONTRACT, WITH RESPECT TO DAMAGES ARISING OR RESULTING FROM ANY ACTION OR

	CLAIM OF SUPPLIER'S BREACH OF SUPPLIER'S CONFIDENTIALITY, PRIVACY, SECURITY OBLIGATIONS UNDER THE CONTRACT (INCLUDING ANY BREACH OF THE DATA PROCESSING AGREEMENT OR ANY BUSINESS ASSOCIATE AGREEMENT ENTERED BETWEEN THE PARTIES), AND SUPPLIER'S DATA SECURITY INCIDENT INDEMNITY OBLIGATIONS AS SET FORTH IN SECTION 16.1 OF THE CONTRACT, SUPPLIER'S TOTAL AGGREGATE LIABILITY WILL NOT EXCEED TWENTY MILLION DOLLARS ($20,000,000 USD) (THE "SUPERCAP")." FOR AVOIDANCE OF DOUBT, NO PROVISION OF THIS CONTRACT SHALL BE CONSTRUED TO NEGATE OR OTHERWISE RENDER UNENFORACABLE THE SUPERCAP APPLICABLE TO ANY OF SUPPLIER'S OBLIGATIONS AS IDENTIFIED IN THIS SECTION, INCLUDING, BUT NOT LIMITED TO, SUPPLIER'S DATA SECURITY INCIDENT INDEMNITY OBLIGATIONS, AS IDENTIFIED IN SECTION 16.1 E.
Attachment B, Section 19	Notwithstanding anything to the contrary in the Contract, the State acknowledges and agrees that in shall not be entitled to terminate any of the Services (with the exception of Professional Services) for convenience. As such, Section 19 (Termination for Convenience) of Attachment B to the Contract and Section 5 (Termination for Convenience) of Attachment C to the Contract, and any other references to termination for convenience in the Contract, are hereby deleted in their entirety.
Attachment B, Section 6, Ordering, Inspection and Acceptance	The following is added as 6.5: The parties agree and understand that Supplier will provide quotes to Customer for a term of 12 months or as otherwise agreed to between parties.

Section	Exception/Notes
Attachment D, Section 1.9	The definition of “Security Incident” in Section 1.9 is hereby amended by deleting the reference to “attempted or” therein.
Attachment D, Section 2	The first sentence of Section 2 of Attachment D is hereby modified by adding the following language to the beginning thereof: “Solely to the extent not provided as part of the Supplier’s Cloud Services (i.e., provided at no additional cost),”
Attachment D, Section 5	Notwithstanding anything to the contrary in the Contract (including but not limited to Section 5 of Attachment D (Offshore Services), the State hereby consents to the Supplier subcontracting all or part of the Services to its Affiliates and to any of the permitted sub-contractors, and the accompanying processing locations, as set forth in the Cover Page to the Contract and in Attachment E-6 (Support Services Description).
Attachment D, Section 6.2	Section 6.2 is hereby amended by adding the following language at the end of the first sentence therein: “or similar industry standard.”
Attachment D, Section 9	Section 9 (Source Code Escrow) is not applicable to the Services being provided pursuant to the Agreement and should be deleted in its entirety, along with any other references to Source Code Escrow set forth in the Contract.
Section 12 and any other relevant Sections of Attachment D	Notwithstanding anything to the contrary in the Contract, and except as expressly agreed otherwise in an Order, Professional Services are limited to implementation and configuration support relating to the Cloud Service and shall in no event be considered a “works made for hire” engagement. The parties hereto acknowledge and agree that at the time of execution of the Contract, Supplier: (i) does not create deliverables as part of its normal business practices; (ii) is not providing hardware or the physical installation of hardware, equipment, computers, and/or the purchase, delivery, transportation and/or support

	thereof; (ii) is not providing bespoke software or software development, or any custom software at the State's request. In the event that the parties mutually agree that the Supplier should ever create or deliver any of the aforementioned items for the State pursuant to the Contract, the parties agree to enter into a separately executed writing to govern such agreement. Therefore, all provisions of the Contract relating to such items which are not applicable to the Services provided under this Agreement, including but not limited to the Information Technology Terms set forth in Attachment D to the Contract (including references in Sections 1.11, 1.13 and Section 12 - Intellectual Property Ownership), shall be deleted in their entirety and will become applicable only upon written agreement by the parties.
Attachment D, Section 14	Section 14 (Change Management) is hereby deleted in its entirety and replaced with the following: "Scheduled Maintenance times for the Cloud Service will be posted on the status.celonis.com. Supplier will endeavor to provide times at least forty-eight hours prior posting of any scheduled maintenance for the Cloud Service. In addition, updates will be uploaded to Supplier's SaaS infrastructure approximately four times per year. This may cause short breaks in the availability of the service as well. Supplier will inform the State about such updates in advance."
Attachment D, Section B (3) of Appendix 1	The last sentence of Section B (3) is hereby deleted in its entirety and replaced with the following new sentence: "Should the virus propagate to Customer's IT Infrastructure as the result of Supplier's breach of its obligations in this Section B (3), Supplier shall be responsible for actual costs incurred by Customer for Customer to remediate the virus."
Attachment D, Section B (4) of Appendix 1	Section B (4) of Appendix 1 to Attachment D is hereby amended by adding the following language to the beginning of the first sentence in Section B(4): "Except as otherwise provided in the Cover Page to the Contract and in Attachment E-6 (Support Services Description), or as otherwise agreed in writing by the State,". Section B(4) of Appendix 1 to Attachment D is hereby further amended by deleting the second sentence in

	Section B (4) in its entirety.
Attachment D, Section B (5) of Appendix 1	Section B (5) of Appendix 1 to Attachment D is hereby amended by adding the following to the end of Section B (5): "Any such audit shall be performed no more than once per annum, upon 30 days' prior written notice to Supplier, and subject to the confidentiality obligations set forth hereunder or separate confidentiality agreement. Such audit shall be conducted during normal business hours and shall be limited to audit Supplier's conformance with its information and data security obligations set forth under the Contract and shall be handled on a remote basis unless otherwise agreed to by the parties."
Attachment D, Section D (4) of Appendix 1	Section D (4) of Appendix 1 to Attachment D is hereby amended by deleting the Section in its entirety and replacing it with the following new language): "In the event of a confirmed Data Breach, Supplier shall provide notice to Customer within 24 hours (unless shorter time is required by applicable law), but failure to do so is not a material breach of the agreement. Where the notification to the Customer is not made within 24 hours, it shall be accompanied by reasons for the delay. Furthermore, if Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall take commercial reasonable measures to address the Data Breach in a timely manner." "Reasonable belief of a Data Breach shall mean that the facts and circumstances would lead Supplier to objectively conclude that there is a reasonable likelihood of a Data Breach."
Attachment D, Section G (1) of Appendix 1	Section G (1) of Appendix 1 to Attachment D of the Contract is hereby amended by adding the following language to the end of Section G (1) as follows: "Notwithstanding anything to the contrary in the Contract, Supplier's sole liability (and the State's

	exclusive remedy) for any breach of the foregoing warranty in this Section G(1) shall be as specified in Section 16.2 (relating to an Infringement Claim) of Attachment B (as amended)."
Attachment D, Section G of Appendix 1	Section G of Appendix 1 to Attachment D to the Contract is hereby amended by adding the following language to the end of Section G: "EXCEPT AS EXPRESSLY PROVIDED IN THE CONTRACT, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. Notwithstanding anything to the contrary in the Contract, SUPPLIER DOES NOT DISCLAIM THE WARRANTY OF NON-INFRINGEMENT."
Attachment D, Section H of Appendix 1	Section H of Appendix 1 to Attachment D to the Contract is hereby deleted in its entirety. The parties agree to defer to Attachment B, Section 16 (as amended) as the centralized location for any Indemnification Obligations.
Attachment D, Section I (3) of Appendix 1	Section I (3) of Appendix 1 is hereby deleted in its entirety and replaced with the following new Section 1(3): "Customer Data shall be available to the Customer for export or download at any time during the Subscription Term. Within 30 days of the termination or expiration of Customer's Subscription, Supplier will delete or destroy any Customer Data then in Supplier's possession unless applicable law requires retention for a longer period. Any retained data is subject to the confidentiality provisions of the Contract.

THE INFORMATION SECURITY POLICY INFORMATION SECURITY POLICY, PROCEDURES, GUIDELINES (THE "POLICY", as REFERENCED IN ATTACHMENTS D AND D-1)

Section	Exception/Notes
Attachment D-1, Section 2	Section 2.d.xi. of Attachment D-1 is hereby deleted in its entirety.
Section 2.3(3)(C) of the Policy	The State hereby acknowledges and agrees that the obligations set forth in Section 2.3(3) (C) of the Policy do not apply to Supplier as a contractor providing Services under this Contract.
Section 2.4(2)(B) of the Policy	The following supplements Section 2.4(2)(B), where applicable to Supplier: i. For internal Celonis accounts, passwords will expire in a maximum of 120 days. For Celonis customers this is not set by default, and Customer can set this control in place by implementing an external identity provider like SMAL2.0 or OpenID Connect.
Section 2.4(2)(D) of the Policy	The following supplements Section 2.4(2)(D), where applicable to Supplier: i. For internal Celonis accounts, Supplier maintains a record of the previous ten (10) passwords used by Users, and Users are not allowed to repeat any such passwords. For Celonis customers this is not set by default, and Customer can set this control in place by implementing an external identity provider like SMAL2.0 or OpenID Connect.
Sections 2.5 and 7.3(1)(E) of the Policy	The following supplements Section 2.5 and Section 7.3(1)(E), where applicable to Supplier: i. Supplier shall ensure that any Customer Data is appropriately backed-up. Supplier does not provide archiving capabilities. As the data controller and owner of Customer Data, Customer can export Customer Data at any time or up to 30

	days after expiration or termination of the Subscription Term, or longer if a longer time period is required by law.
Section 3.5(2) of the Policy	The following supplements Section 3.5(2), where applicable to Supplier: i. Supplier does not provide archiving options for the Cloud Service. Celonis customers have complete control over their data, including logs which can be exported at any time for up to 30 days after expiration or termination of the Subscription Term. User-facing audit logs are built into the Cloud Service, and Customer can export or forward the logs automatically to Customer's own SIEM using Celonis APIs.
Section 5.0 of the Policy	The State hereby acknowledges and agrees that the obligations set forth in Section 5.0 of the Policy do not apply to Supplier as a contractor providing Services under this Agreement.
Sections 7.5-7.8 of the Policy	The State hereby acknowledges and agrees that the obligations set forth in Sections 7.5 through 7.8 of the Policy do not apply to Supplier as a contractor providing Services under this Agreement.
Section 8.2(5) of the Policy	The State hereby acknowledges and agrees that the obligations set forth in Section 8.2(5) of the Policy do not apply to Supplier as a contractor providing Services under this Agreement.
Section 9 of the Policy	The following supplements Section 9 where applicable to Supplier: i. Supplier uses third-party hosting providers to host its Cloud Service, and as such, references to a physical data center do not apply to Supplier. All hosting of Customer Data shall be within the geographical limits of the United States.

Appendix E to the Policy	The State hereby acknowledges and agrees that the obligations set forth in Appendix E to the Policy do not apply to Supplier as a contractor providing Services under this Agreement.

Attachment F-1 to
STATE OF OKLAHOMA CONTRACT WITH CELONIS, INC.
RESULTING FROM SOLICITATION NO. 0000000199

Template for Contract Modifications for Quotes, Statements of Work, or other Ordering Documents

The parties agree to use this template as the process to formally approve any terms, conditions or clauses that are to supersede the terms and Conditions in the Contract for purposes of the applicable quote, statement of work or other ordering document.

Contract Modifications for Quote, Statement of Work, or other Ordering Document

Solely for purposes of this ordering document, the terms and conditions of the Contract are hereby amended as set forth below. This amendment is considered an Addendum.

RFP Section	Exception/Additional Terms

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND
ENTERPRISE SERVICES

By: ________________________________

Name: ______________________________

Title: ________________________________

Date: ________________________________

CELONIS, INC.

By: ________________________________

Name: ______________________________

Title: ________________________________

Date: ________________________________

The [INSERT AGENCY NAME] is additionally executing this document to memorialize its involvement in negotiation of and its agreement with the terms of this document.

By: ________________________________

Name: ________________________________

Title: ________________________________

Date: ________________________________