OKLAHOMA
Office of Manageme
& Enterprise Service

State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA STATEWIDE CONTRACT WITH JUNIPER NETWORKS

This State of Oklahoma Statewide Contract ("Contract") is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and Juniper Networks ("Supplier") in connection with Oklahoma Statewide Contract No. 1006 and Solicitation # 0900000506 and is effective as of the date of last signature to this Contract. The term of this Contract is for one (1) year and there are four (4) one-year options to renew the Contract which the parties may exercise via signed, written agreement.

Purpose

The State is awarding this Contract to Supplier for the provision of Juniper's full catalog of Network Products and Services to the State as articulated in the Contract Documents attached herein.

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 # 0900000506, Attachment A;
   2.2. General Terms, Attachment B;
   2.3. Statewide 1006J-Specific Terms, Attachment C;
   2.4. Information Technology terms, Attachment D;
      i. State of OK Hosting Agreement, Attachment D, Ex-1;
   2.5. Portions of the Bid, Attachment E;
      i. Attachment E, Ex-1 Juniper MPLA;
      ii. Attachment E, Ex-2 Juniper Pricing;
      iii. Attachment E, Ex-3 Juniper Customer Data Protection;
      iv. Attachment E, Ex-4 Juniper Shipping Terms; and
   2.6. Negotiated Exceptions to Contract, Attachment F.

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.

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: ______________________

Name: D. Jerry Moore

Title: Chief Information Officer

Date: Jun 17, 2022

JUNIPER NETWORKS

By: Tim Bunting
Tim Bunting (Jun 16, 2022 16:51 EDT)

Name: Tim Bunting

Title: Assistant General Counsel

Date: Jun 16, 2022

Approved by OMES Finance FC

ATTACHMENT A

SOLICITATION NO. 0900000506

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 the full catalog of Juniper products and services.

1. **Contract Term and Renewal Options**
   The initial Contract term, which begins on the effective date of the Contract, is one year and there are [4] one-year options to renew the Contract.

2. **Certain Contract requirements and terms are set forth below as Exhibit 1.**

Attachment A,

Exhibit 1

Scope of Work

1. **PPRODUCTS AND SERVICES**
   1.1. Supplier must provide the full catalogue of Juniper products and services.
   1.2. Services in support networking equipment may include but are not limited to:
      1.2.1.maintenance,
      1.2.2. technical services (may include, but are not limited to),
         1.2.2.1. hardware
         1.2.2.2. installation
         1.2.2.3. configuration
         1.2.2.4. design
         1.2.2.5. warranty
         1.2.2.6. maintenance services
         1.2.2.7. repair
      1.2.3. managed services (may include, but are not limited to), and
         1.2.3.1. management of Customer owned equipment or
         1.2.3.2. a defined set of services to Customer.
      1.2.4.training

2. **E-RATE - UNIVERSAL SERVICE FUND DISCOUNT**
   2.1. To the extent the services offered are subject to the E-rate discount program, all award Contract Suppliers must commit to participation in the Federal Communication Commission's E-rate discount program established under authority of the Federal Telecommunications Commission Act of 1996.
   2.2. Participation in, and implementation of, this program must be provided without the addition of any service or administration fee by the Contract Supplier.
   2.3. In order to participate in E-Rate Suppliers must appear on the USAC website as those who have a Service Provider Identification Number or "SPIN."E-rate applicants must deduct the value of ineligible components bundled with eligible services unless those ineligible components qualify as "ancillary" to the eligible services under FCC rules. This process is called "cost allocation". Supplier must separate and illustrate the cost allocation for each component and service in a bundled offering provided to E-rate eligible State entities enabling each entity to properly apply for E-rate coverage of allowable services.
   2.4. The Supplier shall not currently be subject to the Red Light Rule by the FCC, and will notify the applicant if they are later placed on Red Light Status with the FCC.
   2.5. The Supplier must be able to honor the applicant's request for Service Provider Invoicing. Service Provider Invoicing is a billing arrangement where the Supplier invoices the applicant for the discounted portion of the products and services the applicant requests.
   2.6. The Supplier should invoice USAC for the non-discounted portion of the applicant's products and services as a reimbursement.
   2.7. Products sold in the E-rate category do not carry the state's administrative fee cost as part of Attachment C, section 6.

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 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. 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 https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. 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
5005 North Lincoln Boulevard, Suite 300

Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel 5005
North Lincoln Boulevard, Suite 300 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://omes.ok.gov/sites/g/files/gmc316/f/isd_itas.pdf. 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 https://omes.ok.gov/s/g/files/gmc316/f/InfoSecPPG_0.pdf.

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 http://eclipse.omes.ok.gov.

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

Reserved.

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

Reserved.

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

<u>With a copy, which shall not constitute notice, to:</u>
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	

HOSTING AGREEMENT

This Hosting Agreement (“Hosting Agreement”) is a Contract Document in connection with the Contract issued as a result of Solicitation No. ___________________________ (the “Contract”) and entered into between ______________________ (“Vendor”) and the State of Oklahoma by and through the Office of Management and Enterprise Services (“State” or “Customer”), the terms of which are incorporated herein. This Hosting Agreement is applicable to any Customer Data stored or hosted by Vendor in connection with the Contract. Unless otherwise indicated herein, capitalized terms used in this Hosting Agreement without definition shall have the respective meanings specified in the Contract.

I. Definitions

a. “Customer Data” shall mean all data supplied by or on behalf of Customer in connection with the Contract, excluding any confidential information of Vendor.

b. “Data Breach” shall mean the unauthorized access by an unauthorized person that results in the access, use, disclosure or theft of Customer Data.

c. “Non-Public Data” shall mean 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.

d. “Personal Data” shall mean 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) contains electronic protected health information that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended.

e. “Security Incident” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the hosted environment used to perform the services.

II. Customer Data

a. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Vendor 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. Vendor 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).

b. Vendor 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. Vendor 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, Vendor shall not respond to subpoenas, service or process, FOIA 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 Vendor's proposed responses. Vendor agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

c. Vendor 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 Vendor. Vendor will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Vendor will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Vendor as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Vendor's negligence or willful misconduct, Vendor, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

III. Data Security

a. Vendor 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. Vendor 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 Vendor applies to its own personal data and non-public data of similar kind.

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

c. Vendor represents and warrants to the Customer that the hosting equipment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Vendor will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Vendor 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 Vendor, Vendor 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 Vendor has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Vendor is responsible for costs incurred by Customer for Customer to remediate the virus.

d. Vendor 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. Vendor 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. Vendor shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Vendor's obligations under the Contract.

e. Vendor 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.

f. Vendor 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. Vendor 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.

IV. Security Assessment

a. The State requires any entity or third-party vendor hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Vendor 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.

b. To the extent Vendor requests a different sub-contractor than the third-party hosting vendor already approved by the State, the different sub-contractor is subject to the State's approval. Vendor agrees not to migrate State's data or otherwise utilize a different third-party hosting vendor in connection with key business functions that are Vendor's obligations under the Contract until the State approves the third-party hosting vendor's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party hosting vendor does not meet the State's requirements under the State Certification and Accreditation Review, Vendor acknowledges and agrees it may not utilize such third-party vendor in connection with key business functions that are Vendor's obligations under the Contract, until such third party meets such requirements.

V. **Security Incident Notification and Responsibilities**: Vendor shall inform Customer of any Security Incident or Data Breach

a. Vendor 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, Vendor will coordinate with Customer prior to making any such communication.

b. Vendor 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).

c. Vendor shall: (i) maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to Customer at Customer's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Vendor; and
(iv) documents all Security Incidents and their outcomes.

VI. **Data Breach Notification and 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 Vendor.

a. Vendor, unless stipulated otherwise, shall promptly notify the Customer identified contact within 2 hours or sooner, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a Data Breach.

Vendor 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.

b. Unless otherwise stipulated, if a Data Breach is a direct result of Vendor's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Vendor 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 – (2), (3) and (4) 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 Vendor based on root cause.

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

VII. **Notice:** Contact information for Customer for notifications pursuant this Hosting Agreement are consistent with the Contract with a copy sent to:

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

And

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

OMES Information Services General Counsel 3115
N. Lincoln Blvd
Oklahoma City, OK 73105

<u>For immediate notice which does not constitute written notice:</u> OMES
Help Desk

405-521-2444
helpdesk@omes.ok.gov
Attn: Chief Information Security Officer

VIII. Vendor Representations and Warranties: Vendor represents and warrants the following

a. The product and services provided under this Hosting Agreement do not infringe a third party's patent or copyright or other intellectual property rights.

b. Vendor 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.

c. The execution, delivery and performance of the Contract, the Hosting Agreement and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Vendor 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 Vendor and any third parties retained or utilized by Vendor to provide goods or services for the benefit of the Customer.

d. Vendor 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.

IX. Indemnity

a. Vendor's Duty of Indemnification. Vendor agrees to indemnify and shall hold the State of Oklahoma and State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees) (collectively "Damages") (other than Damages that are the fault of Customer) arising from or in connection with Vendor's breach of its express representations and warranties or other obligations in this Hosting Agreement and the Contract. If a third party claims that any portion of the products or services provided by Vendor under the terms of the Contract or this Hosting Agreement infringes that party's patent or copyright, Vendor shall defend and indemnify the State of Oklahoma and

Customer against the claim at Vendor’s expense and pay all related costs, damages, and attorney’s fees incurred by or assessed to, the State of Oklahoma and/or Customer. The State of Oklahoma and/or Customer shall promptly notify Vendor of any third party claims and to the extent authorized by the Attorney General of the State, allow Vendor to control the defense and any related settlement negotiations. If the Attorney General of the State of Oklahoma does not authorize sole control of the defense and settlement negotiations to Vendor, Vendor shall be granted authorization to equally participate in any proceeding related to this section but Vendor shall remain responsible to indemnify Customer and the State of Oklahoma for all associated costs, damages and fees incurred by or assessed to the State of Oklahoma and/or Customer. Should the software become, or in Vendor’s opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated under this Hosting Agreement, Vendor 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.

X. Termination and Suspension of Service:

a. In the event of a termination of the Contract, Vendor shall implement an orderly return of Customer Data in a mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of Customer Data.

b. During any period of service suspension, Vendor shall not take any action to intentionally erase any Customer Data.

c. In the event of termination of any services or agreement in entirety, Vendor shall not take any action to intentionally erase any Customer Data for a period of:

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

   ii. 30 days after the effective date of termination, if the termination is for convenience

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

   After such period, Vendor shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

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

e. Vendor shall securely dispose of all requested data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer. 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.

IMPORTANT -- READ THIS AGREEMENT BEFORE ACCESSING OR USING ANY JUNIPER HARDWARE, SOFTWARE, CLOUD SERVICES OR SERVICES.

YOU SHALL HAVE NO RIGHT TO ACCESS OR USE ANY JUNIPER PRODUCTS OR SERVICES UNLESS (I) YOU RECEIVED SUCH PRODUCTS OR SERVICES FROM JUNIPER OR ANOTHER APPROVED SOURCE AND (II) YOU CONSENT TO BE BOUND BY ALL TERMS OF THIS AGREEMENT, WHICH CONSENT IS EVIDENCED BY ANY OF THE FOLLOWING: CLICKING A BOX INDICATING ACCEPTANCE; ACCESSING OR USING JUNIPER PRODUCTS OR SERVICES; OR EXECUTING AN AGREEMENT OR ORDER FORM THAT REFERENCES THIS AGREEMENT.

IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "COMPANY" AND/OR "END USER" (AS APPLICABLE) IN THIS AGREEMENT SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT ACCESS OR USE JUNIPER PRODUCTS OR SERVICES.

MASTER PURCHASE AND LICENSE AGREEMENT

This Master Purchase and License Agreement (the "**Agreement**") is entered into between Juniper and the party accepting these terms ("**Company**" or "**End User**") (each individually, a "**Party**", and collectively, the "**Parties**"), and consists of the General Terms and Conditions set forth below, the Online Policies, Guidelines and Procedures, and the following Schedule(s) and/or Special Terms attached to the General Terms and Conditions, all of which are incorporated, as applicable, into this Agreement by this reference:

- Channel Schedule: Terms and Conditions Applicable to resellers only;
- End User Schedule: Terms and Conditions Applicable to End Users only;
- Glossary: The glossary of defined terms; and
- Special Terms: Supplemental terms and conditions applicable to specific transactions, including, but not limited to, Agency Terms, System Integrator Terms, or Federal Terms.

GENERAL TERMS AND CONDITIONS

1. Scope. These General Terms and Conditions ("**GTC**") set forth terms and conditions for the purchase and/or licensing of Hardware, Software, Services, and/or Cloud Services by the Company during the Agreement Term.

2. Precedence. In the event of any conflict, the following documents that are listed higher in order have precedence and apply in place of any substantially similar terms and conditions of a document lower in the order:

- State of Oklahoma Contract # 1006J, as negotiated by the parties;
- The GTC and the Glossary;
- The terms and conditions of the applicable Schedule;
- The terms and conditions of any applicable Special Terms;

- The terms and conditions of an attachment to one of the above;
- The terms and conditions of Descriptive Content; and
- The terms and conditions of any Online Policies, Guidelines and Procedures.

3. Term. This Agreement is effective from the date of Company's acceptance (the "**Effective Date**") and will have an initial term until the twelve (12) months immediately following the Effective Date ("**Initial Term**").

4. Transactional Terms.

The following terms apply as indicated within the applicable Schedule(s).

a) Payment. All payments due hereunder must be made net forty-five (45) days from the date of invoice. Juniper may require other payment arrangements and may further require a credit check. Unless otherwise stated herein, payments shall be made in U.S. dollars. Accounts past due are subject to a monthly charge of 1.5% or the maximum amount permitted by law, whichever is less, based on the outstanding overdue balance.

b) Ordering. Company must comply with the Purchase Order Requirements. Company's non-compliance with the Purchase Order Requirements may result in Juniper's rejection of Company's Purchase Order. Juniper will confirm its ability to meet Company's requested delivery dates or propose alternative dates. The planned delivery date is referred to as the "**Scheduled Delivery Date**."

c) Cancellations and Rescheduling. Unless revisions are required by Juniper, Company may not cancel, reschedule, or otherwise modify Purchase Orders, in whole or in part, less than thirty (30) days prior to the Scheduled Delivery Date. Should a request for a cancellation or rescheduling received thirty (30) days or less prior to the Scheduled Delivery Date be approved by Juniper (in its sole discretion), the Hardware, Software, Cloud Services and/or Services will be subject to an order cancellation charge equal to ten percent (10%) of the purchase price.

d) Delivery. Except for purchases made indirectly through Authorized Resellers, Company understands and agrees that the terms below in this Section, as supplemented by the additional delivery terms posted in the Shipping Terms Exhibit as set forth at Exhibit A (the "**Shipping Terms Exhibit**"), are the sole and exclusive terms of delivery and supersede all additional or inconsistent terms of any Purchase Order or other ordering document.

e) Taxes. All prices payable under this Agreement are exclusive of Taxes and are paid net of any applicable withholding tax. The Company shall be responsible for paying Taxes arising from purchases of Hardware, Software, Cloud Services and/or Service. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing. The Company shall: (i) promptly notify Juniper if its exemption is revoked or modified; (ii) render reasonable assistance to Juniper by promptly providing valid tax receipts and other required documentation of the payment of any withholding taxes; (iii) promptly provide any applications for reduced tax rates; and (iv) promptly notify and assist Juniper in any audit or tax proceeding, related to transactions hereunder; (v) comply with all applicable tax laws and regulations; and (vi), fully indemnify, defend and otherwise pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of the Company's non-compliance or delay with its responsibilities herein. Neither party shall be liable for taxes or assessments on the other Party's net income, gross income, capital, net worth, franchise, privilege, property, or any similar taxes or assessments.

5. Reserved.

6. Confidentiality

a) Scope. "Confidential Information" means all information disclosed, directly or indirectly, to the other party (the "**Receiving Party**") and labeled as confidential or proprietary, stated at the time of oral disclosure to be confidential or proprietary. Confidential Information does not include information which: (i) is or becomes generally known through no fault of the Receiving Party; (ii) is known to the Receiving Party at the time of receipt, as evidenced by the Receiving Party's records; (iii) is hereafter furnished to the Receiving Party by a third party as a matter of right and without restriction on disclosure; or (iv) is independently developed, as evidenced by contemporaneous records by the Receiving Party without use of or reference to such Confidential Information.

b) Protection. The Receiving Party will use a reasonable degree of care to maintain all Confidential Information to accomplish the purposes of this Agreement or as otherwise agreed in writing by the disclosing Party. The Receiving Party will not disclose to any third party nor use Confidential Information for any unauthorized purpose. The Receiving Party may only disclose Confidential Information: (i) to its employees and representatives that have a need to know to accomplish the purposes of this Agreement; and (ii) in response to a valid order of a court or other governmental body or as otherwise required by law to be disclosed, provided the Receiving Party, to the extent legally permissible, gives sufficient notice to the disclosing party to enable the disclosing party to take protective measures. Except as otherwise expressly set forth in this Agreement, no rights or licenses to intellectual property in Confidential Information is granted by either Party under this Agreement, whether express, implied or otherwise, to the other Party. The obligations imposed on the Receiving Party shall survive the expiration or termination of this Agreement.

c) Injunctive Relief. In the event of a threatened or actual breach of this Section 6, the non-breaching party shall be entitled to seek immediate injunctive or other equitable relief, in addition to, and not in lieu of, any other available remedies.

7. Data Protection. All data collected, processed, and/or used in connection with this Agreement is subject to the Juniper Privacy Policy. Juniper shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of End User Data as described in the User Guides and/or the applicable Documentation. To the extent End User Data includes Personal Data, as defined in the Data Protection Agreement ("**DPA**") located at Attachment E, Ex-3 the terms of the DPA are hereby incorporated by reference and shall apply.

8. Intellectual Property. Subject to the express rights and licenses granted by Juniper in this Agreement, Company acknowledges and agrees that: (i) any and all intellectual property rights in or to the Hardware, Software, Services, and/or Cloud Services are the sole and exclusive property of Juniper or its licensors; (ii) Company shall not acquire any ownership interest in any such intellectual property rights under this Agreement; and (iii) if Company acquires any intellectual property rights in or relating to any product or Services sold or licensed under this Agreement (including any rights in any derivative works or patent improvements relating thereto), by operation of Law, or otherwise, such rights are deemed and are hereby irrevocably assigned to Juniper, without further action by either Party.

9. Reserved

10. Reserved

11. Reserved

12. Warranty Disclaimer. Except as expressly set forth in this Agreement, and to the extent permitted by applicable Law, Juniper (on behalf of itself and its Affiliates) EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH REGARD TO THE HARDWARE, SOFTWARE, SERVICES, AND CLOUD SERVICES, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY RIGHTS, ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE, AND ALL WARRANTIES THAT THE HARDWARE, SOFTWARE, SERVICES, OR CLOUD SERVICES WILL MEET THE REQUIREMENTS OF COMPANY OR ANY OTHER PERSON OR ENTITY, BE AVAILABLE OR OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, OR BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, PRODUCT, OR SERVICE.

13. Reserved

14. Services Suspension and Termination Rights. Except for Cloud Services, Juniper may suspend any unpaid Services with thirty (30) days' notice to the Company. Where the Company continues to be in default, Juniper may in addition to any other remedy, terminate those Services with or without notice to Company (or to any End User) in which case, Juniper will have no liability for ceasing the Services.

15. Miscellaneous

a) Governing Law. This Agreement shall be interpreted and governed by the laws of the State of Oklahoma without regard to its conflict of laws principles or to the U.N. Convention on Contracts for the International Sale of Goods, the application of which is hereby excluded. For any disputes arising out of this Agreement, the Parties consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Oklahoma County, Oklahoma.

b) Compliance with Laws; Export Requirements.

Company and its personnel shall always comply with the Compliance Rules.

In the course of Company's purchase, resale, or use (as applicable) of Hardware, Software, Cloud Services and/or Services, Company shall comply strictly with all export and import laws, if applicable. In addition, Company shall fulfill the additional duties regarding export and import controls and trade sanctions as described in the applicable sections of the Export Notes attached as part of the Shipping Terms Exhibit

Company shall not directly or indirectly export, re-export, transfer, divert, release, or import Hardware, Software, Cloud Services and/or Services, to any other person or entity (nor make any use thereof) except with all required government approvals, permits, and licenses or as otherwise permitted under U.S. and other applicable Laws. Without limiting the foregoing, Company shall not export or re-export, directly or indirectly, any Hardware, Software, Cloud Services and/or Services to any Group E country (currently Syria, Cuba, Iran, North Korea) (Supp 1 to EAR Part 740) or the region of Crimea.

c) Reserved

d) Assignment. Reserved..

e) Notices. Any notices related to this Agreement must be in writing and sent by registered mail or receipted courier service, in the case of: (i) Juniper, to the Address Details; and (ii) the Company, to the address provided by the Company. Juniper may permit other notification methods as described in the Onboarding Information. Notices may also be posted on the relevant Juniper website.

f) Audit. Company will maintain accurate and legible records for a period of three years after the termination or expiration of the Agreement, and will grant to Juniper, or its designee, reasonable access to and copies of, any information reasonably requested by Juniper to verify compliance with the terms of this Agreement.

g) Severability; Remedies; Waiver. In the event that any one or more provisions contained herein shall be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions contained herein shall not in any way be affected or impaired. Except as otherwise expressly provided herein, the remedies contained herein are cumulative and in addition to any other remedies at law or equity. A Party's failure to enforce any provision of this Agreement shall not constitute a waiver of any future enforcement of that or any other provision of this Agreement.

h) No Third-Party Beneficiaries. With the exception of Section 2 (e) of the End User Schedule, this Agreement does not constitute a third party beneficiary contract and, unless expressly and specifically stated in this Agreement, shall not be construed to be for the benefit of any person or entity not a party hereto, and no such person or entity shall have any license, right, or claim in connection with this Agreement.

i) Guidelines and Policies. Juniper may at any time modify any Online Policies, Guidelines and Procedures effective when posted to the applicable site, provided that no such modification shall affect the provision of Hardware, Software, Cloud Services and/or Services under any Purchase Order accepted by Juniper prior to the effective date of such modification. By ordering Hardware, Software, Cloud Services and/or Services under this Agreement, Company understands that it is bound by Juniper’s then-current version of its Online Policies, Guidelines and Procedures.

j) Entire Agreement; Amendment. Reserved.

16. The English Version of Agreement Governs

The English language version of this Agreement constitutes the entire understanding and contract between the Parties and supersedes all prior agreements, commitments or representations between the Parties, whether oral or written, as well as any downloaded or translated version of this Agreement, whether or not such downloaded or translated version is signed (including by digital or other electronic means) by either Party. Any copy of this Agreement made by reliable means (for example, photocopy or facsimile) is considered an original.

END USER SCHEDULE

(Applies to all of End User’s purchases of Hardware, Software, Cloud Services and/or Services for internal use)

1. Scope of Agreement. This End User Schedule is between Juniper and the End User that licenses the right to use the Software and/or access the Cloud Services, and purchases the Hardware and/or Services as part of a solution (collectively, "**Juniper Solutions**"), either (i) directly from Juniper, and/or (ii) indirectly through Authorized Resellers, solely for internal use and not for resale. The applicable sections below will govern the licensing and/or purchase of the applicable Juniper Solutions.

2. Terms for all Juniper Solutions

a) Transactional Terms. Section 4 of the GTC applies to direct Orders only and does not apply to End User orders from an Authorized Reseller.

b) Pricing. Unless purchasing or licensing via an Authorized Reseller, or as otherwise negotiated on a deal by deal basis and set forth in a Quote or Purchase Order acknowledgement, the purchase price for the Hardware, Software, Cloud Services, and/or Services is as set forth in the pricing information submitted to the State of Oklahoma by Juniper in its RFP response and included in the Contract.

c) Use of Third Party Products / Applicable Terms. For non-Juniper branded products and/or services delivered in connection with this End User Schedule, such third-party products and/or services shall be separately governed and licensed by the applicable third-party product and/or services terms and conditions. Such third-party terms and conditions shall supersede this End User Schedule for non-Juniper branded products and/or services. For the avoidance of doubt, the third-party supplier of non-Juniper branded products and services shall be solely responsible for support, warranties, indemnities and other terms and conditions applicable to such products and services.

d) End of Life / End of Service. Juniper will provide End of Life ("**EOL**") and End of Service ("**EOS**") notifications to End User for discontinued Hardware, Software, Cloud Services, and/or Services, either directly or through an announcement posted on the Juniper website, in accordance with Juniper's EOL/EOS Policies.

e) Third Party Licensors. To the extent that Juniper has embedded any third party software or components in any Juniper Solution, that third party licensor may enforce its license rights against the End User under the terms of this Agreement.

f) End of Entitlement. Upon cessation of the right to Use of Software or Cloud Services, End User shall promptly permanently delete, destroy or return all copies of the Software and any Confidential Information to Juniper, and End User shall, provide written certification that it has complied with this paragraph 2(f), if requested by Juniper.

3. Specific Terms for Hardware

a) Hardware Warranty Policy. The terms and conditions of the Juniper Product Warranty are available at Attachment E, Ex-4.

b) Title Transfer. If End User decides to transfer title to its Juniper Platform, then it must remove all Software and/or Embedded Software before transferring title. All transferred Juniper Platforms and subsequent Software licensing are subject to the Service and Support Inspection and Reinstatement Policy.

4. Specific Terms for Services

a) Support Services (Maintenance Services, Advanced Services, Education Services). The following terms in this Section constitute the End User Support Agreement ("**EUSA**") as referred to in the applicable Descriptive Content.

i. Service Term. Subject to Juniper's acceptance of a valid Purchase Order from End User or an Authorized Reseller, the term of the applicable Service Contract will begin on: (1) the date of Purchase Order acceptance if the Purchase Order does not include the associated Hardware (if any) or the Service Contract is for Software only; (2) the date the Hardware is deemed delivered by Juniper if the Purchase Order for the Service Contract includes associated Hardware; or (3) the date as agreed to in writing between the Parties (including as quoted by Juniper and listed in the Purchase Order), if any, in which event such date shall supersede any date determined under (1) or (2).

ii. Renewal Term. The start date of the Service Contract following the initial Services term of the Services (and any subsequent renewal terms) will beginupon a specified date contained in a signed writing by the parties. This Contract does not automatically renew at any point.

iii. Renewal Process. The parties may renew this Contract upon a signed, written agreement.

iv. Subcontracting. Juniper may subcontract with, or assign to, its Affiliates or other third parties the obligations for performance of any Services provided Supplier adheres to all applicable assignment and subcontractor requirements articulated here and elsewhere in the Contract.

v. Descriptive Content. Scope and details of Support Service-specific terms are specified in the applicable Descriptive Content that is attached to or referred to in a Schedule or Quote, or is made available through the then-current Juniper website. The version of the applicable document that is effective as of the date of the applicable Quote, shall be deemed incorporated by reference into the Purchase Order.

vi. True Up. End User must promptly True Up any unpurchased Support Services rendered by Juniper.

b) Professional Services. End User may request on an "as-needed", non-exclusive basis Professional Services. Where Juniper agrees to provide such Professional Services the Parties will mutually agree on a SOW, which shall include at a minimum: (i) a reasonably detailed description of the project or Professional Services to be performed; (ii) a schedule and completion date; (iii) the position description of who will perform the applicable Professional Services; (iv) an acceptance procedure for the Professional Services rendered; (v) a compensation and payment schedule; and (vi) the identity of the End User who will receive the benefit of the Professional Services. Where the Professional Services are provided to End User through an Authorized Reseller, the Authorized Reseller will deliver such services under a SOW as agreed between End User and such Authorized Reseller.

i. End User Obligations. End User: (1) shall be responsible for the accuracy and completeness of the information End User provides to Juniper; (2) agrees to provide all necessary direction and cooperation to enable Juniper to provide the Professional Services; and (3) agrees to provide instructions in a manner reasonably requested by Juniper and Juniper shall be entitled to act on any such instructions, whether provided verbally, electronically, or in writing by a person known to Juniper and that Juniper reasonably believes to be authorized to act on End User's behalf or End User's designee.

ii. Juniper Obligations. Juniper: (1) will not be responsible for any delays or liability arising from missing, delayed, incomplete, inaccurate or outdated information provided by End User, or if End User does not provide adequate access to its employees, agents, and other representatives necessary for Juniper to perform the Professional Services; and (2) represents and warrants that the Professional Services will be provided in a professional and workmanlike manner and performed in accordance with generally accepted industry standards; and (3) will be solely responsible for securing suitably trained and experienced personnel to perform Professional Services hereunder.

5. Specific Terms for Software and Cloud Services

a) License and Right to Use. Subject to the terms and conditions of this End User Schedule, Juniper grants End User a non-exclusive, non-transferable (subject to Section 5 b) below): (i) license to Use the Software, and (ii) right to Use the Cloud Services, during the License Term and/or Subscription Term, as applicable, for up to the Licensed Units. Licenses or rights to Use the Software and/or Cloud Services that are not expressly granted in this End User Schedule shall not arise by implication or otherwise and are hereby expressly reserved. End User shall have no right or license in the Software, nor a right to Use the Cloud Services, unless End User rightfully acquired the Software or purchased the right to Use the Cloud Services from an Approved Source. Unless expressly authorized by Juniper, Use of the Software and/or Cloud Services may not exceed the Licensed Units for such Software and/or Cloud Services.

b) General Restrictions. Unless expressly authorized by Juniper, or except to the extent transfer may not be legally restricted under applicable Law, End User shall not sublicense, transfer, or assign, whether voluntarily or by operation of law, any right or license in or to the Software and/or Cloud Services to any other person or legal entity, including an End User Affiliate, even if End User transfers title to the Juniper Platform or when a lease to any Juniper Platform ceases. Any such attempted sublicense, transfer, or assignment shall be void. Further, End User shall not: (i) directly or indirectly, decompile, disassemble, reverse engineer, modify, unbundle, detach or separate any part of or embed within, or create derivative works based on, any Software and/or Cloud Services; (ii) sell, resell, rent or lease any Software and/or Cloud Services; (iii) unless expressly authorized by Juniper, make any copies of Software and/or Cloud Services except as reasonably necessary for archival and "cold" back-up purposes, but not for failover or "warm" back-up purposes; (iv) remove (or, if the license includes the right to make copies of the Software, fail to include in those copies) any readme files, notices, disclaimers, marks, or labels included in or on the Software and/or any Juniper Platform as delivered by Juniper or any Juniper Authorized Reseller; and (v) Use or allow Use of the Software or Cloud Services in violation of any applicable Law or to support or facilitate any illegal activity.

c) Fulfillment Email and License Activation. To download purchased Software, or Use Cloud Services, End User must register with Juniper by name as the end user of the Software or Cloud Services. Juniper will send a Fulfillment Email to End User’s email that is registered with Juniper or as provided by the End User on the Purchase Order. Juniper shall not be liable for acts and omissions of the Authorized Reseller, including but not limited to, the Authorized Reseller’s failure to include End User’s proper email address on the Purchase Order to Juniper. The Fulfillment Email will provide End User, or the Authorized Reseller, with details on how to activate and Use the Software or Cloud Services that End User has purchased.

d) Subscription Term. The applicable Subscription Term will be listed in the SKU. The Subscription start date will commence on the date of the Fulfillment Email. The Subscription will end at the expiration of the Subscription Term. Unless agreed to in writing, the Subscription will not automatically renew. For any new Subscription: (i) new Subscriptions can be purchased at any time, provided that such purchases are not for retroactive coverage; and (ii) upon End User’s timely renewal of a Subscription, the start date of End User’s renewed Subscription Term will be the day following the expiration of its then-current Subscription Term.

e) Expired Subscription Renewals. For all Subscriptions that have lapsed: (i) Subscription renewals will be backdated to the day following the end of the expired Subscription term; and (ii) after a thirty (30) day lapse, access to the Software and/or Cloud Services may be disabled, Cloud Service functionality may be reduced or limited to read only access, and/or End User's right to Use will be revoked. If access is disabled due to a lapse of thirty (30) days, then End User must purchase a new Subscription to resume the Cloud Service. Expired Subscription renewals are subject to the Service and Support Inspection and Reinstatement Policy.

f) Non-Commercial Purposes/Trial Terms. Software or Cloud Services that are licensed for non-commercial purposes, including but not limited to trial, demonstration, education, or for End User's internal testing and lab purposes ("**Non-commercial Purposes**") are provided by Juniper "AS IS WITH ALL FAULTS AND WITHOUT EXPRESS OR IMPLIED WARRANTIES, CONDITIONS, OR REMEDIES and shall be offered free of charge until the earlier of: (i) cancellation of the free trial of Software or Cloud Services in Juniper's sole discretion and without notice; (ii) expiration of the free trial of Software or Cloud Services, time-limited by Juniper under additional trial terms; (iii) if applicable, the Client Software, is no longer a supported release under an active Service Contract under the terms of this End User Schedule or, to the extent applicable, an accepted agreement for Software support and Maintenance Services between End User and Juniper; or (iv) the start date of any purchased Software or Cloud Services ordered by End User. In no event shall Juniper have any obligation to continue nor any obligation to renew any Software License or Cloud Service Subscription used for Non-commercial Purposes. Software and/or Cloud Services that have been licensed for Non-commercial Purposes shall not be Used in a production environment. Additional trial terms and conditions may appear on an applicable Juniper registration web page. Any such additional terms and conditions are incorporated into this End User Schedule by reference and are legally binding.

g) Federal Government End User Provisions. The Software and Cloud Services herein constitute "commercial items" and include "commercial computer software" and "commercial computer software documentation." Pursuant to Federal Acquisition Regulations 12.211 and 12.212 or Defense Federal Acquisition Regulation Supplement 227.7102-1 and 227.7202-3, as applicable, and Department of Defense transactions DFAR 252.227-7015, as applicable, the U.S. Government shall have only the license rights in technical data, computer software, and computer software documentation specified in this Agreement, and no Authorized Reseller may agree to grant End User any rights in Juniper's technical data inconsistent with this Agreement. Any provisions within this Agreement that are inconsistent with federal procurement regulations are not enforceable against the U.S. Government. If a government agency has a need for rights not conveyed under these terms, it must negotiate with Juniper to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

h) Data Protection. In connection with End User's use of Software and/or Cloud Services, Juniper collects and uses Processed Data in accordance with the Juniper Privacy Policy. By using the Software and/or Cloud Services, End User agrees to allow Juniper to collect and use Processed Data as contemplated in this Agreement.

i) Software Warranty and Performance. The terms and conditions of the Juniper Product Warranty applicable to Software are available at Attachment E, Ex-4. During the Subscription Term, Juniper will provide the Cloud Services with commercially reasonable care in material conformance with the Documentation and Descriptive Content.

6. Supplemental terms for Software

a) Scope. The terms in this Section apply solely to End User's licensing of Software.

b) Software Use. End User may Use the Software on any device that supports it, EXCEPT: (i) Software under an Embedded Software License; (ii) for operating system Software that is licensed and purchased separately from the Juniper Platform, which, assuming such operating system Software is under an effective warranty or Maintenance Services agreement, may only be Used on a replacement Juniper Platform (obtained from Juniper or an Authorized Reseller) in the event of a Hardware failure (with prompt written notice to Juniper); (iii) for Software and its Updates that End User accesses through a Commercial Cloud Service provider acting as an Authorized Reseller or other Juniper-authorized Commercial Cloud Service provider, in which case End User shall be entitled to access and Use only such Software Instance(s) as may be provisioned for End User in the Commercial Cloud Service environment and End User's right to Use shall be solely through the Commercial Cloud Service; or (iv) as otherwise agreed to in a written amendment to this End User Schedule or as set forth in any custom terms between the Parties).

c) Software Updates. Juniper grants End User a license and right to use, solely during the Perpetual License term or Subscription Term, Updates made available as part of Maintenance Services contracted for such Software license or Juniper Platform (for Embedded Software Licenses and its associated Feature Set Licenses), for up to the Licensed Units. Each Update, if any, shall be subject to the same terms and conditions as the Software to which such Update pertains.

d) Source Code. In the limited event that licensed Software includes source code, such source code is provided for reference purposes only unless expressly licensed otherwise by Juniper or its licensors.

e) Perpetual Licensing. Subject to End User's compliance with the terms of this End User Schedule, Software with a Perpetual License will be licensed to End User for a perpetual License term. The perpetual License term will commence on the date that: (i) for Embedded Software or bundled Software with a Hardware component, the Hardware component is delivered; or (ii) in all other cases, Juniper sends End User the associated Fulfillment Email.

f) License Compliance Management. End User shall track its Use of Juniper Software in order to True Up unlicensed use and/or use of a specific Juniper Licensing model. Such tracking may be managed by: (i) the Juniper Agile Licensing ("**JAL**") License Manager tool; (ii) a successor tool provided by Juniper; or (iii) by End User's manual tracking.

g) Java Trademark Guidelines. End User must: (i) comply with the Java Trademark Guidelines; (ii) not do anything harmful to, or inconsistent with, the rights of the Java Rightsholder; and (iii) assist the Java Rightsholder in protecting and restoring its rights, to the extent that the Software contains Java.

h) Use of Software with Third Party Cloud Services. End User's right of access and Use of the Software as part of a third party cloud service is subject to the ongoing validity and compliance with the applicable third party cloud service terms of use imposed by the third party cloud service provider. Termination, suspension, or unavailability of the third party cloud service is at End User's own risk and End User acknowledges that Juniper shall have no liability or duty arising out of any such termination, suspension or unavailability. For purposes of clarity, if End User uses the Software with a Juniper Cloud Service, then such Cloud Service will be subject to Section 7 of this Schedule below.

7. Supplemental terms for Cloud Services

a) Cloud Service Subscriptions. If End User purchases Cloud Services, Juniper will provide End User with a Subscription for non-perpetual Cloud Services, that includes Support Services as defined in the applicable CSD. Juniper reserves all rights, title and interest in and to the Cloud Services, including all related intellectual property rights. No rights are granted to End User hereunder other than as expressly set forth herein.

b) End User's Responsibilities. End User shall: (i) require its Users' compliance with this End User Schedule; (ii) if applicable, be solely responsible for the accuracy, quality, integrity and legality of End User Data and of the means by which End User acquired End User Data; (iii) prevent unauthorized Use of the Cloud Services, and notify Juniper promptly both orally and in writing of any such unauthorized Use; (iv) Use the Cloud Services only in accordance with the User Guides, CSDs, and applicable Laws; (v) obtain any and all third party consents necessary for the use and processing of End User Data in connection with Cloud Services as contemplated in this Agreement; (vi) if applicable, maintain the supported release of the Client Software and also maintain the Juniper Hardware and/or Software, if any, connected with the Cloud Service under the terms of the applicable Descriptive Content; and (vii) Use the Cloud Services with only appropriately licensed and/or Juniper approved third party software and technology. If the Cloud Service is made available as a feature of a Juniper Solution, the Juniper Solution(s) is/are not provided as a part of the Cloud Service and must be purchased separately from Juniper or an Authorized Reseller. Unless the Cloud Service is a security Cloud Service, to the extent that the Cloud Service includes security features and functionalities, End User will not rely on the Cloud Service as End User's network's sole, complete, or timely source of protection from network security threats, including but not limited to, Malicious Code.

c) Additional Cloud Service Restrictions. End User shall not: (i) authorize or allow any person's or entity's direct or indirect access to the Cloud Services (or Use the Cloud Services) other than a User or Users acting for End User's sole benefit in furtherance of End User's internal business operations; (ii) Use the Cloud Services with third party products other than those for which the Cloud Services were purchased or otherwise intended to be used with the Cloud Services, as provided by Juniper in any of the applicable Documentation; (iii) Use the Cloud Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights; (iv) Use the Cloud Services to store or transmit Malicious Code (except to the extent that the Cloud Services include malware scanning, security screening or other threat detection features, such as the option for End User to submit custom threat feeds); (v) interfere with or disrupt the integrity or performance of the Cloud Services or third-party data contained therein; (vi) attempt to gain unauthorized access to the Cloud Services or their related systems or networks; (vii) permit any third party to access the Cloud Services except as permitted herein; or (viii) allow any individual, entity or organization to gain access to the Cloud Service if End User knows, or has reason to believe, that such individual, entity or organization is (or is acting on behalf of) either: (1) any individual, entity or organization identified as a sanctioned party on any list maintained and published by the U.S. Department of Treasury, Office of Foreign Asset Control, or on any similar list of sanctioned parties published by an agency of the US, the EU or any member country of the EU; or (2) an entity or organization 50% or more controlled, directly or indirectly, by a party so listed.

Juniper reserves the right, without liability, to disable End User's access to the Cloud Services in the event of any material breach by End User or its Users or anyone on End User's behalf, of the provisions set forth in this Section.

d) Network Connection. End User shall be solely responsible for procuring and maintaining End User's network connections and telecommunication links from End User's systems to Juniper's servers from which the Cloud Services are accessed. End User shall be solely liable for problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to End User's network connections or telecommunications links, or internet connection.

e) Cloud Service Subscription Activations. For Cloud Services that are purchased as part of a Juniper Solution that includes Hardware, or purchased as standalone Cloud Services, the Subscription Term begins upon delivery of the Fulfillment Email to End User.

f) Cloud Service Subscription Cancellations. Pre-paid Subscriptions to Cloud Services are non-cancellable and non-refundable unless such cancellation is due to Juniper's uncured breach of these terms of this End User Schedule, in which case End User shall be entitled to a pro-rata refund taking into account the remaining term of such Cloud Services at the time of such cancellation.

g) Cloud Services Provided Through Software. Depending upon the Cloud Service purchased, as described within the applicable User Guides, the Cloud Services may be provided through licensed Software which is subject to the End User Software licensing terms in this End User Schedule.

h) Descriptive Content. The scope and details of Cloud Service-specific terms are specified in the applicable Descriptive Content that is attached to or referred to in a Schedule and/or Quote or is made available through the then-current Juniper website. The version of the applicable document that is effective as of the date of the applicable Quote, shall be deemed incorporated by reference into the Purchase Order.

GLOSSARY

A. Definitions applicable to the General Terms and Conditions

"Address Details" means the Juniper corporate address as set forth at https://www.juniper.net/us/en/contact-us/corporate-counsel/, but does not include any email address (if listed).

"Advanced Services" means the resident engineer services and resident consulting services, as well as other services posted at https://support.juniper.net/support/guidelines/ and provided by Juniper.

"Affiliate" of a party means, any entity and its successors controlled by, controlling, or under common control with, such party, where "control" in any of the foregoing forms means ownership, either direct or indirect, of more than 50% of the equity interest entitled to vote for the election of directors or equivalent governing body. An entity shall be considered an Affiliate only so long as such entity continues to meet the foregoing definition.

"Agreement" has the meaning set forth in the Preamble.

"Agreement Term" has the meaning set forth in Section 3 of the GTC.

"Authorized Reseller" means a reseller of Juniper Hardware, Software, Services and/or Cloud Services that sells Juniper Hardware, Software, Services and/or Cloud Services contracts to End Users pursuant to a valid contract with Juniper to conduct such resale activities.

"Business Partner Code of Conduct" means the code of conduct which is located and accessible at http://www.juniper.net/assets/us/en/local/pdf/additional-resources/business-partner-code-of-conduct.pdf.

"Channel Schedule" means the terms and conditions applicable to Authorized Resellers only.

"Cloud Services" means online services provided over the Internet by Juniper to which Sections 5 and 7 of the End User Schedule applies.

"Codes" means: (a) Juniper's Business Partner Code of Conduct; and (b) any other policies, guidelines or references that Juniper makes available to Company from time to time.

"Company" means the Party referenced in the Preamble purchasing and/or licensing Hardware, Software, Services and/or Cloud Services from Juniper hereunder.

"Compliance Rules" means: (a) Laws; (b) any legislation or regulation with respect to anti-bribery, anti-slavery, anti-corruption (including the U.S. Foreign Corrupt Practices Act and the UK Bribery Act) or anti-terrorism; and (c) any Codes.

"Confidential Information" has the meaning set forth in Section 6 of the GTC.

"CSD" or "Cloud Service Description" means a Cloud Service Description, including but not limited to: the incorporated Support Services with any Cloud Service, Juniper's obligations in providing the Cloud Service, and Cloud Service specific privacy and data protection information posted at http://www.juniper.net/support/guidelines.html and referencing this Agreement as governing terms for the Cloud Services described therein.

"Descriptive Content" means materials, documentation, and information that describes the Hardware, Software, Services, and/or Cloud Services as made available by Juniper from time to time, and includes "Data Sheets," "Service Description Document(s)," or "Cloud Service Description(s)".

"Documentation" in any form whatsoever, means any Juniper manuals, materials, guides, specifications, tables, charts, diagrams, pictures, schematics, plans, methods, reports or testing procedures, and any information required for training or education purposes and includes any updates, changes, or derivatives of any of the foregoing.

"DPA" has the meaning set forth in Section 7 in the GTC.

"Education Services" means training and education services provided by Juniper.

"Effective Date" has the meaning set forth in Section 3 in the GTC.

"End User" means the person or organization that originally purchases, leases or licenses Hardware, Software, Services and/or Cloud Services from Juniper or an Authorized Reseller for use in such person's or organization's own business operations and not for further distribution or sale.

"End User Data" means all information submitted by Company to Juniper and may include third party data that Company submits to Juniper.

"End User Schedule" means the terms and conditions applicable to End Users only.

"Hardware" means the physical components of Juniper's equipment delivered in connection with this Agreement.

"Indemnitees" has the meaning set forth in Section 9 of the GTC.

"IP Claims" has the meaning set forth in Section 10 of the GTC.

"Juniper " means, if Hardware, Software, Services and/or Cloud Services are shipped, rendered, delivered or deployed by Juniper or an Authorized Reseller to a location in: (a) North America, Central America or South America, Juniper Networks (U.S.), Inc; (b) United Kingdom, Juniper Networks (U.K.) Limited; (c) India, Juniper Networks Solution India Private Limited; (d) Australia, Juniper Networks Australia Pty Ltd; or where a location is not listed above, Juniper Networks International B.V., and in the case of on-site Services, exclusively means the local Juniper Contracting Entity.

"Juniper Contracting Entity" means the Affiliate of Juniper that is the Juniper signatory to the Statement of Work.

"Juniper Privacy Policy" means the Juniper Privacy Policy posted at the following URL: https://www.juniper.net/us/en/privacy-policy/.

"Laws" means laws, ordinances, codes, rules, standards, and regulations of any territory or jurisdiction.

"Maintenance Services" means the technical support services and maintenance provided by Juniper as fully described in the applicable SDD or CSD.

"Onboarding Information" means information that Juniper provides to the Company (as updated from time to time) for the purposes of transacting under this Agreement and, in the case where Company provides information to Juniper, may include End User Data.

"Online Policies, Guidelines and Procedures" means, without limitation, any policies, guidelines, or procedures, that are applicable to any Hardware, Software, Cloud Services, and Services, or that are referenced in this Agreement and that are posted at Juniper's website, www.juniper.net.

"Party" and "Parties" have the meaning set forth in the Preamble.

"Professional Services" means plan, build, migration and optimization services set forth in a Statement of Work.

"Purchase Order" or "Order" means an Order issued to and accepted by Juniper which is fully authorized by a Company representative and subject to the terms and conditions of this Agreement.

"Purchase Order Requirements" means the Purchase Order Requirements located at https://partners.juniper.net/partnercenter/sales/product-ordering/.

"Preamble" means the terms and conditions contemplated before Section 1 of the GTC.

"Quote" means a Juniper quotation issued to the End User or the Authorized Reseller.

"Receiving Party" has the meaning set forth in Section 6 of the GTC.

"Schedule" means the Channel Schedule and/or the End User Schedule attached to these General Terms and Conditions.

"SDD" or "Services Description Document" means a Services Description Document posted at http://www.juniper.net/support/guidelines.html and referencing this Agreement as governing terms for the services described therein.

"Services" means collectively Maintenance Services, Advanced Services, Education Services, and Professional Services.

"Shipping Terms Exhibit" has the meaning set forth in Section 4 of the GTC.

"Special Terms" has the meaning set forth in Section 2 of the GTC.

"Software" means the Juniper machine-readable object code and accompanying activation keys, if any, made available under this Agreement, whether incorporated in the Hardware (e.g., firmware) or delivered separately, and includes Software Releases and any Updates of that Software the End User is entitled to through Maintenance Services.

"Software Release" means a new production version of the Software.

"Statement of Work" or "SOW" means the scope and details of customized Professional Services documented in a mutually agreed to Statement of Work entered into in connection with this Agreement.

"Supported Release" means the version of the Software and certain prior versions of the Software as set forth in Juniper's then current EOL/EOS Policies.

"Tax" or "Taxes" means all taxes, levies, imposts, all custom duties, tariffs, import fees, fines or other charges of whatsoever nature however imposed by any jurisdiction, country or any subdivision or authority thereof in any way connected with this Agreement or any instrument or agreement required hereunder, and all interest, penalties or similar liabilities with respect thereto, except such taxes as are imposed on or measured by a Party's net income or property.

"Update" is defined in the Service Description Document that pertains to the Maintenance Services purchased or included with the Software, as applicable.

B. Definitions applicable to the End User Schedule

"Approved Source" means Juniper or an Authorized Reseller.

"Client Software" means the portion of the Software which enables End User to access, manage or utilize the Cloud Service.

"Commercial Cloud Service(s)" means a service offered and administered by Juniper, or an authorized third party, whereby End User may without downloading or otherwise taking delivery of a copy of the Software use and access Instances of Software running in a virtual machine environment resident in a networked cloud facility or group of facilities.

"Embedded Software" means the operating system Software pre-installed on the Juniper Platform, and is required for the proper functioning of the Juniper Platform and/or for the proper functioning of the cloud services purchased in connection with the Juniper Platform.

"Embedded Software Licenses" means the limited right to Use the Embedded Software and included in the purchase of the Juniper Platform but does not include the right to Use Separately Licensable Features and may not be used in excess of the Licensed Units identified in the SKU for the Juniper Platform. Embedded Software Licenses are Perpetual unless the Juniper Hardware is leased or provided for demonstration purposes, in which case the Embedded Software License term shall follow the lease term or demonstration period and shall terminate automatically upon the expiration of the lease term or demonstration period.

"Embargoed Region" means a country or region subject to comprehensive embargo under US or Netherlands law or regulation or that is classified under US Export Administration Regulations (EAR) as a Group E:1 or E:2 country (see US EAR Supplement No. 1 to Part 740). Regions qualifying under this definition of Embargoed Region as of January 2018 include Cuba, Iran, North Korea, Syria, and the region of Crimea.

"End User Data" means all information submitted by End User to the Cloud Services and may include third party data that End User submits to the Cloud Services.

"EOL/EOS Policies" means policies and guidelines published at https://www.juniper.net/support/eol/# pertaining to product end of life notifications, last order date, end of engineering support, end of support, and like product end of life milestones for Juniper Hardware, Software, Services, and/or Cloud Services.

"Feature Set License" means the limited right to Use solely the certain set of features and functionalities of the Software as described in the Fulfillment Email and SKU, regardless of whether any additional feature or functionality is unlocked and thus accessible to End User in the Software. Feature Set Licenses may also be combined with other Juniper Software licenses.

"Fulfillment Email" means the email document that confirms the End User's purchase of the Software Licenses and/or the Cloud Service for the associated Subscription Term, SKU(s) and, if applicable, contains the activation code or license key, respectively for Software Licenses and/or the Cloud Service, and may be sent by Juniper to (a) the End User directly; or (b) the Authorized Reseller transacting with the End User.

"Instance" means each time the Software runs on any device.

"Java Rightsholder" means Oracle America, Inc.

"Java Trademark Guidelines" are available at http://www.oracle.com/us/technologies/java/java-licensing-logo-guidelines-1908204.pdf.

"Juniper Platform" means any Juniper-provided, but not any third-party-provided, Hardware.

"Juniper Solutions" has the meaning set forth in Section 1 of the End User Schedule.

"License Metric" means a unit of measurement that restricts the scope of use of the Software (e.g., Feature Set License, Instance, Network Element or Node, Session Socket or CPU Socket or Throughput or any other unit of measurement set forth in a SKU) or Fulfillment Email).

"License Term" means the period of time that the Software is licensed to be Used by End User, subject to the terms and conditions of this Agreement.

"Licensed Units" mean a number of units under a License Metric that limits the Use of the licensed Software or use of the Cloud Services (e.g. 10M, 50 Nodes, 1000 Sessions or any other units under a License Metric set forth in a SKU or Fulfillment Email) as set forth in the Fulfillment Email.

"Malicious Code" means viruses, worms, time bombs, trojan horses and other harmful or malicious code, files, scripts, agents, programs, or any identifying information or other metadata associated with them, such as suspected malicious website, URL, or IP addresses.

"Network Element" or "Node" means a physical or virtual device that is recognizable by the Software as a unique device that the Software may directly or indirectly administer, monitor, manage, provision, or configure.

"Non-commercial License" means Software that is used for Non-commercial Purposes.

"Non-commercial Purposes" has the meaning set forth in Section 7.

"Perpetual License" means a license that continues until the first to occur of termination by Juniper or End User's violation of any term or condition of this Agreement, unless such violation is waived in writing by Juniper, and does not include a Subscription License or a Non-commercial License.

"Processed Data" means information about End User's devices or systems generated or otherwise provided in connection with End User's usage of the Cloud Service, as well as any network management information or configuration data generated or otherwise provided from the use of End User's Processed Data with the Cloud Service.

"Separately Licensable Features" means specific features and functionalities of the Software that may only be Used if a Feature Set License is obtained and such features and functionalities are expressly set forth in a SKU) or Fulfillment Email.

"Session" means a stateful information exchange connection established for communication between two devices through a gateway.

"Service and Support Inspection and Reinstatement Policy" means Juniper's Service and Support Inspection and Reinstatement Policy that can be accessed at https://support.juniper.net/support/pdf/guidelines/990222.pdf.

"Service Contract" means a contract for Support Services provided directly by Juniper to the End User as more fully described in the relevant Services Description Document ("SDD") or Cloud Services Description ("CSD") posted at http://www.juniper.net/support/guidelines.html (and any reference to the 'End User Support Agreement or 'EUSA' in a SDD or CSD is a reference to the applicable terms and conditions within this Schedule), and itemized in a Quote and/or Purchase Order as applicable.

"SKU" means a stock-keeping unit or unique identifier for each distinct product and service that can be purchased and any summary description of such product or service associated therewith.

“Socket” or “CPU Socket” means a mechanical component that provides electrical connectivity between a microprocessor and a printed circuit board.

“Subscription” means a license to Use the Software and/or Cloud Services with accompanying Maintenance Services solely during a fixed Subscription Term, unless terminated earlier by Juniper pursuant to the terms and conditions of this Agreement.

“Subscription Term” means the period of time during which a Software subscription or Cloud Services subscription is active, as set forth in the Fulfillment Email.

“Support Services” means collectively Maintenance Services, Advanced Services, and Education Services.

“Throughput” means the maximum possible bits of inbound data traffic capable of being processed per second by an Instance of Software. A Throughput license may not be split across multiple Instances. Throughput licenses will be identified in the SKU description and Fulfillment Email in units of megabits per second (Mbps or M), gigabits per second (Gbps or G), or terabits per second (Tbps or T).

“True Up” means an End User accounting and payment for all deployments or Use of unpurchased or unlicensed Juniper Hardware, Software, Services and/or Cloud Services.

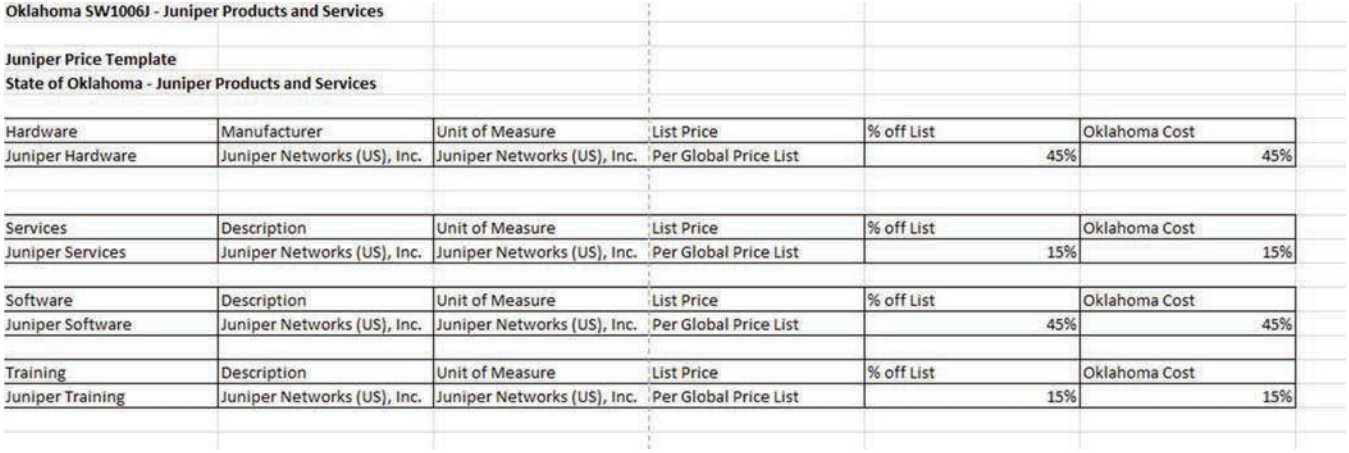
“Update” is defined in the Service Description Document that pertains to the Maintenance Services purchased or included with the Software, as applicable, and any End User rights to Use apply only to the: (a) active or deployed Update; or (b) then-current Update.

“Use” and “Used” means, in the case of: (a) Software, to install, utilize, access, activate, or view the Software in executable form; or (b) Cloud Service, to access or consume that Cloud Service.

“User Guide" means the online user guide, technical guide, data sheets, and/or CSD for the Cloud Services, accessible via a Juniper designated website as updated from time to time.

“Users" means individuals who: (a) are authorized by End User to use on End User’s behalf the Software or Cloud Services for which Subscriptions have been purchased by End User or as part of a free trial; and (b) include, without limitation, end users, employees, consultants, contractors and agents with which End User transacts business.

SECTION NINE: PRICING



Oklahoma SW1006J - Juniper Products and Services

Juniper Price Template
State of Oklahoma - Juniper Products and Services

Hardware	Manufacturer	Unit of Measure	List Price	% off List	Oklahoma Cost
Juniper Hardware	Juniper Networks (US), Inc.	Juniper Networks (US), Inc.	Per Global Price List	45%	45%

Services	Description	Unit of Measure	List Price	% off List	Oklahoma Cost
Juniper Services	Juniper Networks (US), Inc.	Juniper Networks (US), Inc.	Per Global Price List	15%	15%

Software	Description	Unit of Measure	List Price	% off List	Oklahoma Cost
Juniper Software	Juniper Networks (US), Inc.	Juniper Networks (US), Inc.	Per Global Price List	45%	45%

Training	Description	Unit of Measure	List Price	% off List	Oklahoma Cost
Juniper Training	Juniper Networks (US), Inc.	Juniper Networks (US), Inc.	Per Global Price List	15%	15%

ATTACHMENT E, Ex-3 Data Protection and Privacy

Customer Data Protection and Privacy Exhibit for Juniper Products and Services

This Customer Data Protection and Privacy Exhibit for Juniper Products and Services ("**DPA**") supplements the Main Agreement (as may be updated from time to time) and covers the products or services ("**Products and Services**") provided or rendered by Juniper Networks, Inc., 1133 Innovation Way, Sunnyvale, CA 94089, United States and any of its affiliates, as applicable, that may Process Customer Personal Data ("**Juniper Networks**") under a respective end user services agreement or other contract ("**Main Agreement**") between and Juniper Networks and the contracting party receiving Products and Services (as defined in the Main Agreement, hereinafter "**Customer**"), as sold by Juniper Networks or an authorized reseller. This DPA is entered into by and between Juniper Networks and Customer, whether Customer entered into a Main Agreement with Juniper Networks or an authorized reseller.

1. Definitions. Terms used in this DPA shall have the meaning indicated below unless otherwise defined in this DPA.

1.1 "Clauses" shall mean all provisions of this DPA, unless provided otherwise in the relevant context.

1.2 "Customer Personal Data" shall mean the Personal Data described in Schedule 1 of this DPA, in respect of which Customer is the Controller and which is provided to Juniper Networks by or on behalf of Customer and Processed by Juniper Networks, each in connection with the Main Agreement for Juniper Networks to provide Products and Services to Customer.

1.3 "Data Protection Requirements" shall mean any laws or regulations applicable to the Processing of Personal Data or personal information (or similar term under the applicable law or regulation).

1.4 "Member State" shall mean any country within the EU/EEA.

1.5 "Personal Data", "Data Subject", "Process", "Processor", "Controller", and **"Supervisory Authority"** will each have the meaning given to them in applicable Data Protection Requirements.

1.6 "Standard Contractual Clauses" or **"SCC"** shall mean the Standard Contractual Clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or any subsequent version thereof released by the European Commission (which will automatically apply).

Any other terms that are capitalized but not defined below shall have the meanings set forth in Data Protection Requirements and/ or the Main Agreement, as applicable.

2. General Provisions.

2.1. This DPA applies to the Processing of Customer Personal Data. If Data Protection Requirements recognize the roles of "Controller" and "Processor" as applied to Customer Personal Data then, as between Juniper Networks and Customer, Customer acts as Controller and Juniper Networks acts as a Processor (or Subprocessor, as the case may be) of Customer Personal Data. Juniper Networks will only Process Customer Personal Data as a Processor on behalf of and in accordance with Customer's prior written instructions, including with respect to transfers of Customer Personal Data, unless Processing is required by Data Protection Requirements to which Juniper Networks is subject, in which case Juniper Networks shall, to the extent permitted by applicable law, inform Customer of that legal requirement before so Processing that Customer Personal Data. The Parties agree that such instructions are contained in the Main Agreement and that Juniper Networks may Process Customer Personal Data as necessary to enable Juniper Networks to provide the Products and Services according to the Main Agreement. Any additional or different instructions require a signed agreement between Juniper Networks and Customer and may be subject to additional fees. For the avoidance of doubt, Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Requirements. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Personal Data. Juniper Networks will immediately inform Customer if, in its opinion, an instruction from Customer infringes the Data Protection

Requirements, provided, however, Juniper Networks is not responsible for performing legal research and/or for providing legal advice to Customer.

2.2. If Juniper Networks cannot Process Customer Personal Data according to Customer's instructions due to a legal requirement under any Data Protection Requirements, Juniper Networks will promptly notify Customer of such inability, providing a reasonable level of detail as to the instructions with which it cannot comply and the reasons why it cannot comply, to the greatest extent permitted by applicable law.

2.3. Unless set forth in a statement of work, order, or other document, Customer Personal Data may not include any sensitive or special data that imposes specific data security or data protection obligations on Juniper Networks in addition to or different from those specified in any documentation or which are not provided as part of the Products and Services.

2.4. Subject matter and other details of Juniper Networks' Processing are set forth in Schedule 1. Juniper Networks shall Process Customer Personal Data for an indefinite term for as long as the Main Agreement is in effect.

3. International Transfers.

3.1. In accordance with Customer's instructions under Section 2.1, Juniper Networks may Process Customer Personal Data on a global basis as necessary to provide the Products and Services, including for IT security purposes, maintenance and provision of the Products and Services and related infrastructure, technical support, and change management.

3.2. To the extent that the Processing of Customer Personal Data by Juniper Networks involves the transfer of such Customer Personal Data from the European Economic Area ("EEA") to a country or territory outside the EEA, other than a country or territory that has received a binding adequacy decision as determined by the European Commission (an "EEA Transfer"), such EEA Transfer shall be subject to the protections and provisions of the Standard Contractual Clauses (for which the SCC Appendix is attached to this DPA in Schedule 1).

3.3. Customer shall be deemed to have signed the SCC in Annex I in its capacity as "data exporter" and Juniper Networks in its capacity as "data importer." Module Two or Module Three of the SCC shall apply to the transfer depending on whether Customer is Data Controller of the Customer Personal Data (for Module Two) or a Data Processor of the Customer Personal Data on behalf of its end customer(s) (for Module Three). If Module Three applies, Customer hereby notifies Juniper Networks that Customer is a Processor and the instructions shall be as set forth in Section 2.1. For purposes of Clauses 17 and 18 of the SCC, the Parties select The Netherlands. Additional provisions applicable to customer Personal Data transferred pursuant to the SCC and based on the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" are set forth in Schedule 2.

3.4. The SCC will cease to apply if Juniper Networks implements an alternative recognized compliance mechanism for the lawful transfer of Personal Data in accordance with Data Protection Requirements, in which case such alternative mechanism shall apply.

3.5. In the event of any conflict between any terms in the SCC and DPA, the SCC shall prevail to the extent of the conflict.

3.6. If and to the extent there are contradictions or inconsistencies between this DPA and its Schedules, the applicable Schedule(s) shall prevail, unless and to the extent the relevant DPA provision is required under Data Protection Requirements.

3.7. Where Customer Personal Data originating from the United Kingdom specifically is processed by Juniper Networks outside of the United Kingdom, in a territory that has not been designated by the UK Information Commissioner's Office as ensuring an adequate level of protection pursuant to Data Protection Requirements, and to the extent such processing and transfer would be subject to the SCC and Data Protection Requirements applicable in the United Kingdom ("UK Data Protection Requirements") the Parties agree that: (i) general and specific references in the SCC to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 have the same meaning as the equivalent reference in UK Data Protection Requirements; (ii) references in the SCC to a "Member State" mean the United Kingdom and references to a "supervisory authority" shall mean the UK Information Commissioner's Office; and (iii) any other obligation in the SCC determined by the Member State in which the data exporter is established refer to an equivalent obligation under UK Data Protection Requirements.

4. **Bundling of Data Importers.** The parties agree that the bundling of Juniper Networks entities as processors within this single DPA is only undertaken for efficiency purposes (i.e., to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective Customer entity and the Juniper Networks entity and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Juniper Networks entity.

5. **Bundling of Data Exporters.** The parties agree that the bundling of Customer entities, for example, if Customer is comprised of multiple global affiliates, as controllers within this single DPA is undertaken for efficiency purposes (i.e., to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective Customer entity and Juniper Networks solely for purposes of addressing any such obligations under Data Protection Requirements; (ii) shall not create any new or different legal or other relationship whatsoever between the "bundled" Customer entities; (iii) does not create any additional rights or remedies for such bundled Customer entities; (iv) all Processing instructions must be provided by the Customer entity that is signatory to the Main Agreement and Juniper Networks is not responsible for consolidating or evaluating the validity of instructions received from bundled Customer entities; (v) any commercial terms not provided by the DPA are provided by the Main Agreement regardless of whether the bundled Customer entities signed or were consulted regarding the terms of the Main Agreement; and (vi) any audits conducted in accordance with the DPA shall be conducted by and through the Customer entity that is signatory to the Main Agreement.

6. **Data Protection Compliance.** Each party undertakes to comply with the Data Protection Requirements applicable to such party's Processing of Personal Data in connection with the Main Agreement. The Customer as Controller hereby warrants that it has provided all required notices and obtained all permissions or, if applicable and sufficient under Data Protection Requirements, another valid legal basis, required under Data Protection Requirements to provide Juniper Networks with any Personal Data of the Data Subjects specified in Appendix 1 to this DPA or otherwise provided by Customer in connection with the Juniper Products and Services. Customer acknowledges that Juniper Networks is reliant on Customer for direction as to the extent to which Juniper Networks is entitled to Process Customer Personal Data. Consequently, Juniper Networks will not be liable for any claim brought against Juniper Networks by a Data Subject arising from (a) Juniper Networks' actions in compliance with Customer's instructions or (b) any act or omission by Customer in Customer's use of the Products and Services.

7. **Data Secrecy and Confidentiality**. Juniper Networks shall treat the Customer Personal Data Processed as confidential and shall not disclose such data to any third parties unless authorized by Customer and in accordance with this DPA. This obligation continues to apply after the expiration or termination of this DPA for so long as Juniper Networks Processes Customer Personal Data. In accordance with Data Protection Requirements, Juniper Networks shall put procedures in place designed to ensure that all persons acting under its authority entrusted with the Processing of Customer Personal Data (i) have committed themselves to keep such data confidential and not to use such data for any purposes except for the provision of the Juniper Products and Services hereunder, or (ii) are under an appropriate statutory obligation of confidentiality. This obligation to confidentiality shall continue after the end of the respective engagement of such person. Juniper Networks will further instruct such persons regarding the applicable statutory provisions on data protection and shall ensure that access to Customer Personal Data is limited to those persons with a need to know.

8. **Security Measures**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Juniper Networks will implement appropriate technical and organizational measures designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data (described under Annex II to the Standard Contractual Clauses). Juniper Networks may update its security practices from time to time but will not materially decrease the overall security of the Products and Services during the term of a statement of work or other ordering document. Such measures shall include process for regularly testing, assessing and evaluating the effectiveness of the measures.

9. **Subcontracting Authorization.** When subcontracting the Juniper Products and Services or parts thereof to another Juniper Networks entity or a third party, if the subcontractor will Process Customer Personal Data, such subcontractor shall be a Subprocessor and Juniper Networks will enter into a binding written agreement with the Subprocessor that imposes on the Subprocessor the same level of restrictions that apply to Juniper Networks under this DPA, to the extent that such requirements are applicable to the Processing to be done under such subcontract. A list of Juniper Networks Subprocessors is available at https://support.juniper.net/support/subprocessor/index.page ("**Subprocessor List**"). For the avoidance of doubt and in accordance with Clause 9, Option 2 of the Standard Contractual Clauses, the above constitutes Customer's general authorization for Juniper Networks' engagement of Subprocessors and Juniper Networks' appointment of additional Subprocessors or replacement of any Subprocessors identified on the Subprocessor List and in Annex III. In addition to any notifications provided

by Juniper Networks regarding the addition or replacement of Subprocessors or updates to the Subprocessor List, Customer agrees to subscribe to any mechanisms that Juniper Networks may provide for notifications regarding Subprocessors. Customer agrees to provide any objections promptly (in any event no later than fourteen (14) days following any notification or update), provided such objections are based on documented evidence that establish the Subprocessor does not or cannot comply with this DPA or Data Protection Requirements and identify the reasonable data protection basis for the objection (“**Objection**”), so that Juniper Networks can evaluate the Objection and determine any appropriate action. In the event of an Objection, Customer and Juniper Networks will work together in good faith to find a mutually acceptable resolution to address such Objection, including but not limited to reviewing additional documentation supporting the Subprocessor’s compliance with the DPA or Data Protection Requirements.

10. Personal Data Breach Notification.

10.1. Juniper Networks will provide Customer promptly with a data breach notification (with contents detailed below) if Juniper Networks becomes aware of and confirms any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data or any other security incident that compromises the security, confidentiality or integrity of Customer Personal Data that requires a data breach notification to Customer according to Data Protection Requirements (**“Personal Data Breach”**). Customer and Juniper Networks shall work together in good faith within the timeframes for Customer to provide notifications in accordance with Data Protection Requirements to finalize the content of any such notifications to Data Subjects or Supervisory Authorities, as required by Data Protection Requirements. Juniper Networks’ prior written approval shall be required for any statements regarding, or references to, the Personal Data Breach or Juniper Networks made by Customer in any such notifications.

10.2. As information regarding the Personal Data Breach becomes available for Juniper Networks to disclose to Customer, Juniper Networks will provide Customer with information regarding (1) the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Personal Data records concerned; (2) the reasonably anticipated consequence of the Personal Data Breach; (3) summary of measures taken to address or mitigate any possible adverse effects; and (4) other information concerning the Personal Data Breach reasonably known or available to Juniper Networks that Customer is required to disclose to a Supervisory Authority or Data Subjects under Data Protection Requirements. Juniper Networks’ contact point for additional details regarding a Personal Data Breach is privacy@juniper.net. Except as required by Data Protection Requirements, the obligations in this Section shall not apply to Personal Data Breaches caused by Customer.

11. Handling of Complaints, Inquiries and Orders. To the extent a Data Subject identifies Customer as the entity that collected its Personal Data, Juniper Networks shall notify Customer of the Data Subject’s complaints and inquiries (e.g., regarding the rectification, deletion and blocking of or the access to Personal Data, or any other rights Data Subject has under Data Protection Requirements) (**“Data Subject Inquiry”**) received by Juniper Networks relating to the Juniper Products and Services covered by the Main Agreement. To the extent Customer, in its use of the Products and Services, does not have the ability to address a Data Subject Inquiry, then at Customer’s expense, Juniper Networks shall provide assistance to Customer to respond to such Data Subject Inquiry in a timely manner. Taking into account the nature of the Processing, Juniper Networks shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of Customer's obligations to respond to Data Subject Inquiry under Data Protection Requirements. Juniper Networks shall not independently respond to Data Subject Inquiries without Customer's prior approval, except where required by Data Protection Requirements. The same shall apply to orders and inquires of courts or regulators. Juniper Networks will instruct Data Subjects that do not identify a relevant Controller to contact the correct Controller. Juniper Networks shall comply with Customer’s instructions regarding the handling of a Data Subject Inquiry, subject to the terms of Section 2.1.

12. Term. The term of this DPA is identical with the term of the Main Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Main Agreement.

13. Data Retention. After the end of the provision of the Products and Services and pursuant to written instructions provided by Customer, Juniper Networks shall return to Customer or securely destroy all copies of Customer Personal Data Processed on behalf of Customer in Juniper Networks’ role as a Processor in connection with the Products and Services. Upon Customer’s written request, Juniper Networks shall provide Customer with a written statement confirming such return or destruction. Juniper Networks may retain Customer Personal Data to the extent required by applicable laws only for such period as required by applicable laws, or as necessary to protect its legal rights, and provided that Juniper Networks shall protect the confidentiality of all such Customer Personal Data and Process such Customer Personal Data only as necessary for the relevant purpose(s) requiring its storage and for no other purpose.

14. **Invalidity and/or Unenforceability.** Should any provision of this DPA be found invalid or unenforceable by a competent court of law, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

15. **Liability.** Indemnification, liability, limitations of liability and any applicable exclusions under this DPA shall be governed by the Main Agreement to the extent permitted by Data Protection Requirements.

16. **Corporate Restructuring**. Juniper Networks may share and disclose Customer Personal Data and other data of Customer in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of Juniper Networks' business by or to another company, including the transfer of contact information and data of customers, partners and end users.

17. **Information, Audits, and Assistance.**

17.1. Upon Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Juniper Networks shall make available to Customer information reasonably necessary to substantiate Juniper Networks' compliance with this DPA. Customer may only use such information to confirm Juniper Networks' compliance with this DPA and to assist Customer with complying with its obligations under Data Protection Requirements. If no such information is available at the time of Customer's request, Juniper Networks will allow and cooperate in audits as set forth below.

17.2. Customer shall have the right to carry out on-site audits (no more than once per year), during regular business hours without disrupting the Juniper Networks' business operations and in accordance with the Juniper Networks' security policies. Any third party engaged by Customer to conduct an audit must be pre-approved by Juniper Networks (such approval not to be unreasonably withheld) and sign Juniper Networks' confidentiality agreement.

17.3. For any audits, Customer must provide Juniper Networks with a proposed audit plan at least two weeks in advance of the audit, after which Customer and Juniper Networks shall discuss in good faith and finalize the audit plan prior to commencement of audit activities. Information obtained or results produced in connection with an audit are Juniper Networks' confidential information and may only be used by Customer to confirm Juniper's compliance with this DPA and to comply with Customer's obligations under Data Protection Requirements.

17.4. If requested by Customer solely in order to support Customer's compliance with Data Protection Requirements, Juniper Networks shall provide, at Customer's expense, reasonably required assistance to Customer in ensuring its compliance relating to data protection impact assessments and prior consultation with Supervisory Authorities, taking into account the nature of the processing and the information available to Juniper Networks. All such information provided shall be Juniper Networks' confidential information.

18. **Amendments for Additional Local Data Protection Requirements.** To the extent that additional country-specific (or state, regional, provincial, or other geographic area specific) provisions are required under Data Protection Requirements, the parties agree to incorporate such provisions solely to the extent they are required and solely to the extent they are applicable to particular Customer Personal Data processed by Juniper Networks. Juniper Networks may, from time to time, post updated provisions related to local or other specific Data Protection Requirements on the Juniper Privacy Policy available at https://www.juniper.net/us/en/privacy-policy under the heading Additional Local Provisions. Such posted provisions are automatically incorporated herein solely to the extent they are required under Data Protection Requirements.

SCHEDULE 1

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data Exporter:
Name: The Data Exporter is the entity identified "Customer" in the DPA.
Address: as set forth in the Main Agreement.
Contact person: as set forth in the Notices provision in the Main Agreement.
Activities relevant to the data transferred under these Clauses: as set forth in the Main Agreement.
Signature and date: refer to DPA.
Role: Controller, except when processing data on behalf of another entity, in which case Data Exporter is a Processor.

Data Importer:
Name: The Data Importer is the entity identified as "Juniper Networks" in the DPA.
Address: as set forth in the Main Agreement.
Contact person: as set forth in the Notices provision in the Main Agreement.
Activities relevant to the data transferred under these Clauses: as set forth in the Main Agreement.
Signature and date: refer to DPA.
Role: Processor, or Sub-processor if Data Exporter is a Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data subjects: The personal data transferred concern the following categories of data subjects:

- Personnel of Data Exporter.
- Personnel of Data Exporter's partners (including any vendors, suppliers, agents or additional subprocessors as may be authorized by Data Exporter).
- Solely to the extent that such data is processed by Data Exporter and shared with Data Importer for processing under the Main Agreement, end users of Data Exporter.

Categories of personal data transferred: The personal data transferred concern the following categories of data in addition to any other categories as specified in: (a) the Main Agreement; (b) the Data Exporter Privacy Policy available at https://www.juniper.net/us/en/privacy-policy/ together with any Supplemental Privacy Information referenced therein (including for Mist Systems) ("**Privacy Policy**"); and (c) in any data sheets or related product documentation provided by Data Importer for the particular product or service ("**Documentation**"):

- Business Contact Data: Business contact information of the data subjects.
- End User Data:
  - Network Devices: Occasionally, Data Exporter or its end users' IP addresses, and less frequently, core dump files or network traffic snippets from a network device, may also be provided when requesting support and could be deemed to contain Personal Data to the extent it can be associated with an individual data subject.
  - Cloud Services: For Data Importer Products and Services that include Cloud services, the categories of data that may be processed are as set forth in the Privacy Policy and Documentation.
  - WLAN: For WLAN Products and Services of Data Importer, such as from its affiliate Mist Systems, Inc., the categories of data that may be processed are as set forth in the Privacy Policy and Documentation.
  - Professional Services: Any personal data that is shared with Data Importer by or on behalf of Data Exporter in connection with any professional services provided by Data Importer under the Main Agreement.

Supplemental Product-Specific Information: Additional information regarding data processing related to particular Products and Services of Data Importer is available in the "**Supplemental Privacy Information**" section of the Privacy Policy.

Sensitive categories of data (if appropriate): The personal data transferred concern the following special categories of data: Data Importer does not require any special categories of data in order to provide its Products and Services. Unless otherwise specified in the Main Agreement, Data Exporter shall not provide and must receive prior written consent of Data Importer before transferring any special categories of data or sensitive data to Data Importer.

The frequency of the transfer: As set forth in the Main Agreement.

Nature of the processing: The personal data transferred will be subject to the following basic processing activities:

> Providing the Products and Services in connection with the Main Agreement, providing related technical support and professional services under the Main Agreement (as applicable), and improving/enhancing such Products and Services and support services.

Data Importer also retains the right to process the Personal Data for purposes including enforcing its legal rights, complying with legal requirements, providing information on Products and Services, training resources, and opportunities for upgrades and enhancements, and other permitted purposes under applicable law, as set forth in the Privacy Policy.

Purposes of the data transfer and further processing: The processing activities defined in Section 2 of the DPA and in the Main Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As set forth in Sections 2.4 and 13 of the DPA, and in the Main Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As set forth in Sections 2.4, 9, and 13 of the DPA, and as set forth in the Main Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

If the Data Exporter is established in an EU Member state, the competent Supervisory Authority shall be the Supervisory Authority applicable to the establishment location of the Data Exporter. If the Data Exporter is not established in an EU Member state, the competent Supervisory Authority shall be the Supervisory Authority located where the Data Exporter has appointed its EU Representative. If the Data Exporter is not established in an EU Member state and is not required to appoint an EU Representative, the competent Supervisory Authority shall be the supervisory authority applicable to the location of the data subject whose data is at issue.

ANNEX II

Technical and organizational measures including technical and organizational measures to ensure the security of the Customer Personal Data:

1. Information Security Governance

- The information security function within Data Importer reports directly to a company executive.
- A Security and Privacy Steering Committee made up of representatives from business, information security, and privacy meets regularly to discuss and review information security policies, projects, and practices.
- A comprehensive set of information security policies and standards are documented, approved, and regularly reviewed.
- Personnel with access to Personal Data are subject to confidentiality obligations.

2. Network Security

- Network security is maintained using industry standard techniques, including, for example, firewalls, intrusion detection systems, access control lists, and routing protocols.
- Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 12 characters with at least three of the following four classes: upper case, lower case, numeral, special character) and be changed periodically.
- WiFi networks are secured and encrypt data in transit. Guests are permitted to connect only to the guest WiFi network and are not allowed to connect to any production systems.
- An intrusion detection or prevention system covers network traffic to the Data Importer information systems.
- Network changes are tested prior to production deployment.
- Firewalls are appropriately configured and implemented. Firewall policies are reviewed on a regular basis.
- Employees and contractors are required to use VPN to connect remotely to the corporate network.

3. Encryption

- Full disk encryption is configured on Data Importer-managed end point devices.
- Encryption methods for Data Importer's systems which Process Data Exporter Personal Data are based on factors such as length of time such data are Processed, technical capabilities of third-party attackers, Data Importer's resources, and sensitivity of the Personal Data.
- Encryption keys to Data Exporter's Personal Data are stored in a key management solution. Keys are rotated periodically and access to keys is restricted to limited personnel with administrative access only. Membership for encryption key ownership groups is regularly reviewed according to a written Encryption Key Management Standard.
- Sensitive Personal Data is encrypted in transit and at rest in compliance with Data Importer's Information Security Cryptographic Policy.

4. Identity and Access Management

- Data processing systems handling Personal Data are subject to measures designed to prevent access, loss or use without authorization.
- Employees or contractors with access to Personal Data are assigned unique IDs.
- Only authorized staff may grant, modify, or revoke access to Data Exporter's Personal Data. The list of authorized staff is regularly reviewed.
- Systems processing personal data are required to integrate with Data Importer's single sign on authentication.
- Access rights are assigned using the principle of least privilege and need-to-know.
- Access is revoked upon termination of the employee or contractor.
- Login attempts are limited and accounts locked after a predetermined number of failed login attempts.
- Remote access for critical applications is controlled via multi-factor authentication.
- Systems processing Data Exporter's Personal Data implement session or screen lockouts after a predetermined period of inactivity.

5. Physical Security

- Physical access to Data Importer buildings by unauthorized personnel is restricted.

- Physical access controls, such as surveillance cameras and identification badges, are implemented for Data Importer's facilities.
- Physical security systems such as fire suppression systems, flood controls, smoke detection, and UPS are utilized.
- Data Importer has implemented significant physical security measures such as perimeter security, access control, CCTV and alarm monitoring, visitor screening and control, security guarding and reception services, and 24-hour Security Operations Centers for monitoring and incident response.

6. Patch and Vulnerability Management

- Anti-malware and anti-virus software are in place and are updated on a regular cadence, including for Data Importer's managed devices handling Personal Data.
- Data Importer implements a patch management program designed to ensure security patches are appropriately applied to systems.
- Vulnerability scans for systems processing Data Exporter's Personal Data are performed on a periodic basis.
- Any known critical vulnerabilities as defined by Data Importer's risk assessment are assessed and remediated in a timely manner.

  Annual penetration tests are conducted for certain Data Exporter-facing systems.

7. Continuous System Monitoring

- Audit logging is implemented in production system. Audit logs are retained for appropriate periods, including as required by applicable regulatory requirements.
- Data Importer reviews and analyses information system audit records for indications of unusual activities.

8. Business Continuity Management

- Emergency and contingency plans are available and maintained in an effort to restore personal data, where applicable, as reasonably deemed appropriate by Data Importer.
- Business continuity plans are tested and updated on a periodic basis, as reasonably deemed appropriate by Data Importer.
- Backups of data are maintained for business continuity purposes, as reasonably deemed appropriate by Data Importer.

9. Incident Response

- Data Importer maintains a written Incident Response plan providing a standard process to investigate and address security incidents and regularly reviews the Incident Response plan.
- Data Importer will notify Data Exporter of Personal Data Breaches in accordance with the DPA and its Breach Notification Plan.
- Data Exporter may contact Data Importer at IT-CIRT@juniper.net for any available details regarding a Personal Data Breach.

10. Security Awareness

- Background checks are required on personnel at the time of hire, to the extent permitted under applicable law.
- Employees are required to undergo periodic privacy and information security training.
- Training is updated as deemed necessary by Data Importer.

11. Third Party Risk Management

- Sub-processors undergo a vendor information security review as appropriate based on their personal data access and are required to comply with vendor security requirements.
- Data Importer has a program to review the information security risk and control of third-party service providers. The review is performed on new and existing vendors. This includes reviews of the effectiveness of the controls of our third-party service providers who process Personal Data, for example through review of their SOC-2 Reports.

12. Secure Development

- Data Importer maintains a secure development program that includes measures such as secure coding practices; use of industry-standard practices to mitigate and protect against vulnerabilities; separate coding environments; source code vulnerability scanning; pre-release source code and application testing; and review of any open source of third-party code prior to its use.

13. Additional and/or Supplemental Technical Security Measures

- Additional and/or supplemental technical security measures, and appropriate modifications to the measures listed above, may be established by Data Importer periodically depending on the Products and Services offered and the type of personal data of Data Exporter that is Processed by Data Importer.
- Data Importer's policy does not permit BYOD or personally-owned devices to process Personal Data provided through the Services.
- In assisting Data Exporter with fulfilling data subject requests, Data Importer shall either (a) provide to Data Exporter an online self-service solution to enable Data Exporter to fulfill data subject requests or (b) otherwise provide reasonable means for Data Exporter to submit requests.
- A change control process is in place for changes to Data Importer production systems.
- Personal Data hosted for different Data Importer customers are logically separated.
- Storage media for customer-facing systems are either destroyed or securely erased at the end of their lifecycle.
- Data Importer incorporates privacy by design and privacy by default practices in its solution development processes.

ANNEX III

List of Data Importer's Subprocessors

As set forth on the webpage https://support.juniper.net/support/subprocessor/index.page.

SCHEDULE 2 – ADDITIONAL SCC PROVISIONS
BASED ON EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS 01/2020

1. Juniper Networks shall, unless prohibited by law or a legally binding order of an applicable body or agency, promptly notify Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) ("Disclosure Request") without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request). Juniper Networks will review applicable law to evaluate any Disclosure Request, for example the ability of the requesting authority to make the Disclosure Request, and will challenge the Disclosure Request if, after a careful assessment, it concludes that there are grounds under applicable law to do so. When challenging a Disclosure Request, Juniper Networks shall seek interim measures to suspend the effects of the Disclosure Request until an applicable court or other authority has decided on the merits. Juniper Networks shall not disclose Customer Personal Data requested until required to do so under applicable law. Juniper Networks shall only provide the minimum amount of Customer Personal Data permissible when responding to the Disclosure Request, based on a reasonable interpretation of the Disclosure Request. If the Disclosure Request is incompatible with the SCCs or other data transfer mechanism utilized in accordance with Section 3 in this DPA, Juniper Networks will so notify the requesting authority and, if permitted by applicable law, notify the competent EEA government authority with jurisdiction over the Customer Personal Data subject to the Disclosure Request. Juniper Networks will maintain a record of Disclosure Requests and its evaluation, response, and handling of the requests. Juniper Networks will provide Customer with such records relevant to Customer Personal Data except as prohibited by applicable law or legal process or in the interest in protecting Juniper Networks' legal rights in connection with threatened, pending, or current litigation.
2. Juniper Networks has not purposefully created "back doors" or similar programming in its systems that provide Products and Services that could be used to access the systems and/or Customer Personal Data, nor has Juniper Networks purposefully created or changed its business processes in a manner that facilitates access to Customer Personal Data or its systems that provide the Products and Services. To the best of Juniper Networks' knowledge, United States Data Protection Requirements do not require Juniper Networks to create or maintain "back doors" or to facilitate access to Customer Personal Data or systems that provide Products and Services or for Juniper Networks to possess or provide the encryption key in connection with a United States Disclosure Request.
3. Juniper Networks shall use reasonable efforts to assist Customer and its Data Subjects, as instructed by Customer (in accordance with Section 11 of the DPA), regarding Disclosure Requests, unless prohibited by applicable law, for example to provide information to Customer in connection with the Data Subject's efforts to exercise its rights and obtain legally-available redress, provided Juniper Networks shall not be required to provide Customer or Data Subjects with legal advice.
4. Customer may request to audit Juniper Networks information regarding access to Customer Personal Data, subject to the terms of Section 17 of the DPA.
5. In the event Juniper Networks receives a request to voluntarily disclose unencrypted Customer Personal Data to a government authority, Juniper Networks will use reasonable efforts to first obtain Customer's consent, either on its behalf or on behalf of the relevant Data Subject.

ATTACHMENT E, Ex-4 Shipping Terms

Shipping Terms / Incoterms / Logistics Value Added Services (L-VAS)

Region	Ship to Location	Incoterms	LVAS / Freight Terms	Delivery Point	Title Transfer	Risk of Loss or Damage Transfers (i.e., Incoterms Delivery Point)	Fee
Americas	USA	FCA Delivery Point	Collect	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	No Fee
		FCA Delivery Point Plus	Prepay & Add	Ship to Address Indicated on PO	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee
		DDP	Economy or Premium / Prepay & Add	Ship to Address Indicated on PO	Availability at Address Indicated on PO	Availability at Address Indicated on PO	Handling Fee
	Canada	FCA Delivery Point	Collect	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	No Fee
		DAP (Import Point)	Economy or Premium / Prepay & Add	Import Point (prior to customs clearance)	Import Point (prior to customs clearance)	Import Point (prior to customs clearance)	Handling Fee
	CALA	FCA Delivery Point	Collect	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	No Fee
EMEA	EU except UK and Non-EU Countries	FCA Delivery Point	Collect	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	No Fee
		FCA Delivery Point Plus	Prepay & Add	Ship to Address Indicated on PO	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee
		*DDP	Economy or Premium / Prepay & Add	Ship to Address Indicated on PO	Juniper Designated Cross Dock	Availability at Address Indicated on PO	Handling Fee
	UK	FCA Delivery Point	Prepay & Add	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee
		FCA Delivery Point Plus	Prepay & Add	Ship to Address Indicated on PO	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee
		DDP	Economy or Premium / Prepay & Add	Ship to Address Indicated on PO	Availability at Address Indicated on PO	Availability at Address Indicated on PO	Handling Fee
	Non - EU Countries	FCA Delivery Point	Collect	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	No Fee
		DAP (Import Point)	Economy or Premium / Prepay & Add	Import Point (prior to customs clearance)	Import Point (prior to customs clearance)	Import Point (prior to customs clearance)	Handling Fee
APAC	All Countries Except AU, MY, VN	FCA Origin (see "Origin" Note below)	Collect	Juniper Designated Origin Site	Juniper Designated Origin Site	Juniper Designated Origin Site	No Fee
	All APAC Countries	FCA Delivery Point	Collect / Prepay & Add	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee for all Countries Except CN, MY, VN
	AU	FCA Delivery Point	Prepay & Add	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee
		FCA Delivery Point Plus	Prepay & Add	Ship to Address Indicated on PO	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Handling Fee
		DDP	Economy or Premium / Prepay & Add	Ship to Address Indicated on PO	Availability at Address Indicated on PO	Availability at Address Indicated on PO	Handling Fee
	IN	FCA Delivery Point	Collect	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Juniper Designated Cross Dock	Inclusive
	All Countries except HK, AU	DAP (Import Point)	Economy or Premium / Prepay & Add	Import Point (prior to customs clearance)	Import Point (prior to customs clearance)	Import Point (prior to customs clearance)	Handling Fee

Notes	AU = Australia, CALA = Caribbean and Latin America Region, CN = China, HK = Hong Kong, IN = India, MY = Malaysia
	Inclusive = For India (IN) shipments on FCA DC Terms, the freight cost for the Logistics Value Added Services (L-VAS) program is included in the prices set for in the India Price List
	All Shipments must be "picked-up" within 48 Hours of notification on FCA Origin, FCA Delivery Point
	"Origin" Note: "Origin" shall be Hong Kong for APACcustomers purchasing product sourced from Juniper's Mexico contract manufacturer and Juniper Direct Fulfillment Center in Milpitas, California. For all other cases, "Origin" will be at a Juniper-designated port near sourcing manufacturer facility.
	*DDP Must have approval from Tax, Legal, and Logistics prior to offering this Incoterm

	* Cross- Dock Locations APAC = Hong Kong
	EMEA= Amsterdam
	UK = London
	IN = India
	AU = Australia
	US = San Francisco, Laredo, El Paso

Version: December 2021

Export Note

In addition to their other duties specified in any agreement that ***Customer***[1] has entered into with Juniper regarding purchase and sale of Juniper ***Products***[2] andServices[3] from Juniper or its resellers, the Juniper and Customer shall fulfill the following additional duties regarding export and import controls and trade sanctions:

1. **Customer Responsibilities.** *(Applies to all Customers)*

   a) General Duty of Compliance, Disclosure and Cooperation. Customer shall comply with all applicable import and export laws relating to the Products, Services and Technology and any Activities associated with them. Customer shall not furnish any false or misleading information to Juniper orto anyone acting on behalf of Juniper and if any information so furnish laterbecomes inaccurate or misleading or incomplete, Customer shall promptly update Juniper with current, complete and accurate information. Customershall promptly and fully cooperate with all requests by Juniper for information, certificates and documentation relating to any Activity involvingProducts, Services or Technology.

   b) Any portion of the items held or stored by Juniper at the designated DC or Origin location after the Delivery Date shall be held at the risk and expense of the Customer. Juniper shall invoice such expenses to the Customer (either the End User or the Juniper Channel Partner, as determined by Juniper in its sole discretion).

2. **Survival**. *(Applies to all Customers)* Customer's duties under this Export Note shall survive termination or expiration for any reason of the Agreementinto which this Export Note is incorporated.

3. **Anti-corruption**. *(Applies to all Customers.)* Neither Customer nor any of itsagents or forwarders shall not offer or give any payments or other consideration directly to or indirectly for the benefit of any government official to induce their clearance of goods or other action or inaction in connection with import or export of Product.

4. **Exportation from shipment origin**. (*Only for End Users (or other Customers)who are Directly Purchasing from Juniper*)

   a) If the incoterms between Juniper and Customer are FCA (a named place)or other "F" Incoterm (Incoterms 2010),

      i) Juniper's responsibilities shall be limited to endeavoring to obtain such export licenses as may be required to Export[4] the Product fromthe FCA named place to the country identified by Customer in its purchase order as the Ship-to address.

      ii) AES filings. For Exports from delivery locations in the US, unless Juniper elects to make AES filings itself, Order Party shall cause itsselected forward to timely file a completed AES submission for all Exports of goods based on information furnished by Juniper in its export invoice for such shipment.

   b) For deliveries under "D" terms, Juniper's responsibilities shall be limited toapplying for such export licenses as may be required to deliver Product tothe Incoterms "named place." For avoidance of doubt, DAT terms do not require Juniper to customs clear the Product into the country in which the named terminal is located.

   c) Juniper shall not be liable for any failure of or delay in delivery

      i) caused by any failure or delay by Customer or any other party to the Activity[5], or to a party's forwarder, in timely fulfilling their duties underthis Export Note, including without limitation the furnishing of current,complete and accurate information regarding the Activity, including without limitation, the name and location of the End User[6] and intended End Use;

      ii) caused by government refusal or delay in issuance of any requiredlicense or in clearance of product out of or into a country.

      iii) caused by non-fulfillment of pre-shipment notifications, certificates or inspections required under license or applicable law due to factors beyond Juniper's reasonable control; OR

      iv) resulting from Juniper's good faith believe that an Export or import compliance violation may occur.

5. **Compliance with Order Management Requirements**. (*Only for End Users(or other Customers) who are Directly Purchasing from Juniper*) Any purchase order placed by Customer with Juniper or with a Juniper distributor:

   i) shall accurately identify the true intended end user of the JuniperProduct or Services being purchased.

   ii) shall identify exactly one End User, and each purchase order must include ONLY Product and Services destined for that identified EndUser; and

[1] "**Customer**" means (i) the party that purchases Product or Services directly from Juniper, in which case such party may be either an End User, or a Juniper Channel Partner (that is, a Juniper-authorized Distributor, Direct VAR, System Integrator, Support Services Specialist or J-Partner reseller) or, (ii) (except where the section is designated "*Only for End Users or other Customers who are Directly Purchasing from Juniper*") a J-Partner reseller that purchases Product or Services from a Juniper-authorized stocking distributor.

[2] "**Product**" means tangible and intangible goods (including, without limitation, network routers, switches, appliances, accessories thereto, parts or components thereof, and end user licenses to software, whether the software is standalone or a module separately licensable or installed or embedded in any hardware) marketed, sold or licensed by Juniper; and any license keys or other access information relating to other Product or features thereof**.**

[3] "**Services**" means maintenance services for Juniper Product (including software updates, replacement and repair of tangible product and technical advice), as well as professional or installation services relating to network installation, configuration, design or administration or operation.

[4] "**Export**" as used herein includes

1. Actual shipment or transmission of an item (including sending or taking an item) from any point (whether in the United States or otherwise) to any country other than the United States;
2. Releasing Technology or software, irrespective of whether by visual or other inspection by a one neither a citizen or permanent resident of the U.S. ("non-US Person") or by oral or written exchanges with a non-US Person or causing release to a non-US person by use of license key, password or other access information, irrespective of whether that non-US Person is in the US or elsewhere;
3. Making the software (or license keys, passwords or other access information relating to such software) available to a non-US person or to a person not located in the US.

[5] **"Activity"** means any sale, delivery, grant of access to, release, subscription, lease, license, or other disposition (and any related series of any kind of such dispositions) of Product,Service or Technology beginning with the sale or lease by a Juniper entity (or Juniper authorized stocking distributor selling from its stock in Juniper Products) through one or more Customers to an End User (defined below). Activity also includes use of the Product and Services and any release of Technology furnished to a Customer by Juniper or its contractors.

[6] **End User**" is the person, entity or other organization or association that will directly or through an agent or contractor operate and use the Products or Services for its own operations and not for resale or other disposition to third parties. The End User is the party that will ultimately put to Product into use or have the Product put to use by its agents or contractors for its benefit. By way of illustration only,

1. A system integrator holding or configuring or using a Product or Service for the benefit of its customer is not an End User.
2. A Customer purchasing with intent to dispose of the Product or Service is not an End User.
3. A purchasing agent acting on behalf of its principal an End User.

iii) shall include the name and address (comprising street address, city,postal code, state or province and country) of the End User (regardless of whether Customer is selling directly to that End User)together with the name and address of any and all other participantsin the Activities by which the Juniper Products or Services will be transferred after resale by Customer through to the End User.

6. Responsibilities of Customers who are Juniper Channel Partners (*Not applicable where Customer is End User*)

a) Export and Import Licenses and Permits.

i) Unless Juniper Trade Compliance otherwise elects by written notice at its sole discretion, Customer shall obtain all necessary governmentlicenses, authorizations and permits with respect to its sale, transport,import, Export, electronic transmission, installation, configuration, update, support and use of Product, Services and Technology. Customer shall also be responsible for fulfilling all conditions and abiding by all restrictions imposed under any applicable license.

ii) Customer's duty includes, without limitation, refraining from diverting any Product or Service or Technology to anyone other than End Useridentified to Juniper at the ship-to location designated in the Customer's purchase order placed with Juniper. It also includes keeping Juniper updated with complete, current and accurate information regarding the identities and locations of all intermediate and final consignees of Product Exported and of all parties to the transaction or series of transactions through to final sale or other disposition to the End User and regarding the end user of the Product.

b) Screening and license determination obligations. Regardless of whether Customer knows or believes that Juniper is aware of the identity of the EndUser, Customer shall diligently verify all relevant facts regarding the Activities and shall not place any purchase order or otherwise participate inActivities if it has any knowledge or any reason to suspect:

i) that the party identified as End User of the product in the purchase order placed with Juniper (or in any certificate or information providedto Juniper in connection with the Activities) might not in fact be the actual ultimate End User of the Products, Services or Technology; or

ii) that any Activity has been or is or might be in violation of US or other applicable export or import laws and regulations, including, without limitation, by virtue of

A) any participant in any Activities in Juniper Product or Services (including, without limitation, the End User) being a SanctionedParty[7]; or

B) any participant in the Activities being a member of any sanctioned sector under US, EU or other applicable export control or economicsanction orders, laws or regulations, including, without limitation, those US and EU sectoral sanctions restricting or prohibiting dealings with military End Users, oil and gas exploration industry orfinancial services industry in Russia[8]; or

C) any participant in any Activities or related series of Activities in Juniper Product or Services (including without limitation the End User) being located in (or intending to use such item for the benefitof anyone located in) or the Product will be shipped or otherwise delivered or transmitted to (or transit (or has transited) through) any country or region listed under the Group E:1 or E:2 country list (Supplement 1 to Part 740 of the US Export Administration Regulations ("EAR")) (currently comprising North Korea, Iran, Cuba, Sudan and Syria) or otherwise subject to comprehensive embargo under US law regulation or order, including the Crimeanregion; or

D) any Products being or having been Exported or imported without allrequired licenses, permits and authorizations under US and all other applicable export and import control orders, laws and regulations; or

E) that end use of any Products, Services or Technology sold, leased,licensed or furnished under the Activities may include

(1) a military end use (unless otherwise expressly agreed by Juniper Trade Compliance Team and Customer in a signedwriting);

(2) development, production, operation or support of nuclear, chemical or biological weapons or missile technology or of nuclear fissile material or facilities for the production of suchmaterial;

(3) a use in connection with violations of human rights, of democratic principles or of the freedom of speech as definedin the Charter of Fundamental Rights of the EU, where use ismade of interception techniques and digital data transfer equipment for monitoring mobile phones and reading text messages and of targeted surveillance of internet use (e.g., by means of monitoring centers and lawful interception gateways); or

(4) that the ship-to address and the address of the End User on Customer's purchase order or the order Customer receives from its customer in connection with the Activities may be a carrier or freight forwarder address or a bonded warehouse orfree trade zone (unless otherwise expressly agreed by Juniper Trade Compliance Team and Customer in a signed writing).

c) Software or license key distribution. Customer shall not make accessible foruse or for electronic download or otherwise electronically distribute any software (or transmit by any means any license keys or other means of access to Products or Product features) to any third party without prior express written consent of the Juniper Networks Trade Compliance team.

d) Support or other Services. Customer shall not render (directly or indirectly through its agents or contractors) Services of any kind unless and until Customer first determines, resolving all reasons to suspect otherwise, that the recipient of those services did not receive the Products that are the subject of such services in an export in violation of any applicable export orimport controls.

e) Other Documentation and Information Required.

i) End User Certificate. If an Activity involves an Export of Product, directly or indirectly, to a High-Risk Country[9], or if Juniper otherwise makes a request on Customer or separately posts a requirement at www.juniper.net, then, at or before placement of its order with Juniper(or in the case of Products shipped under a Stocking Order[10],to a

[7] "**Sanctioned Party**" means (i) any individual, entity or other organization or institution that is named on a list of parties subject to export or economic sanctions published either by US Bureau of Industry and Security ("BIS") (the Denied Persons List, Unverified List or Entity List) (see https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern) or by OFAC (including the SDN list) (see https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx) or by the EU External Action Service (EEAS) or other EU body including the "Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions" (see https://eeas.europa.eu/headquarters/headquarters-homepage/8442/consolidated-list-sanctions_en); or (ii) a party 50% or more owned or controlled, directly or indirectly, by a Specially Designated National (SDN) (as that term is used by US Office of Foreign Asset Control ("OFAC")

[8] US Executive Order 13662 and Directives 1 through 4 thereunder, as amended.

[9] *"**High Risk Country**" means any of the following: Afghanistan, Angola, Belarus, Cambodia, Central African Republic, China, Congo, Egypt, Eritrea, Guinea, Iraq, Laos, Lebanon, Libya, Myanmar, Pakistan, Qatar, Russia, Saudi Arabia, Somalia, South Sudan, Vietnam.*

[10] "***Stocking Order"*** means an order placed by a Juniper–authorized stocking distributor for stock and not for fulfillment of any order placed (or about to be placed) with the Distributor by a Customer.

Customer that is a Juniper –authorized Distributor at or prior to Customer's disclosure to Juniper of the name of End User, but in no event later than date of Customer's shipment or other delivery of anyProduct from Customer's warehouse or other stocking facility), Customer shall obtain and furnish to Juniper a End User Certificate (EUC) in the form found at http://www.juniper.net/us/en/company/citizenship-sustainability/tradecompliance/ signed by the End User.

A) Juniper Trade Compliance may waive this requirement for any particular transaction only in writing and any such waiver shall apply only to the specific Activity involved and not to any other Activity. Such waiver may be made conditional on Customer securing a signed reseller export compliance certificate in a form satisfactory to Juniper attesting to the facts of the Activity and theparties involved, including the End User, and specifying the End Use.

B) Further, unless Juniper Trade Compliance otherwise requests an EUC in writing, the requirement for an End User-signed EUC shallbe waived until lapse of two years from date of delivery to Juniperof the signed EUC.

ii) ELAIS Form. If the End User is a Non-Supplement 3 Country Government End User[11], or if Customer is not selling directly to the End User, then Customer shall also complete and furnish to Juniper (and the Juniper-authorized Distributor from whom Customer is ordering Product), the Juniper-form Export License Application Information Sheet (ELAIS) posted at http://www.juniper.net/us/en/company/citizenship-sustainability/ethics-compliance/ .

f) *Prevent Post-Delivery Diversion*. After Juniper's delivery of goods to Customer, Customer shall be responsible for ensuring that no Product delivered by Juniper is diverted to any party or location not identified on Customer's purchase order, and that transportation of all such Product is handled solely though the freight forwarder designated by Customer on itspurchase order and that no intermediate consignee not named in the purchase order is used in the course of transporting Product to the final destination identified in the purchase order;

g) Collection and Archiving of Documentation. Customer shall:

i) generate and maintain contemporaneously generated businessrecords establishing its compliance with its screening and otherresponsibilities specified in this Export Note.

ii) collect transactional and shipment-related documentation confirming that Product is delivered and received in conformity with terms of thisExport Note through to the End User.

iii) collect complete and current information, certifications, undertakings and other documentation pertaining to transit of Product from point atwhich Juniper delivers Products to Customer through point of End User receipt of Products at final destination. Such documentation shall include, but not be limited to: copies of orders received by Customer for Juniper Products and services, change orders, waybillsand bills of lading, proofs of importation into destination country and proof of delivery to End User, all import or Export licenses relied on in the Activities, proof of compliance with all Export/import licenseconditions, Export and import invoices and declarations.

iv) Archiving. Archive for at least seven (7) years from the date of the Activities and, upon Juniper request, furnish to Juniper

[11] "***Non-Supplement 3 Country Government End User***" is any Government End User acting for a country not in the group of countries comprising the US, Canada, the member countries of the European Union, Norway, Switzerland, Turkey, Iceland, Australia, New Zealand or Japan. "***Government End User"*** as used above is any non-US central, regional or local government department, agency, or other entity performing governmental functions. "Government End User" includes, among other things, governmental research institutions, governmental corporations or their separate business units (as defined in part 772 of the EAR) which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations. "Government End User" does not include utilities (including telecommunications companies and Internet service providers); banks and financial institutions; transportation; broadcast or entertainment; educational organizations (except public schools and universities); civil health and medical organizations (including public civilian hospitals); retail or wholesale firms; and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.

Attachment F to
STATE OF OKLAHOMA CONTRACT WITH Juniper Networks, Inc
RESULTING FROM SOLICITATION NO. 0900000506

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by **Juniper Networks, Inc.** or discussed by the parties.

ANY REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE.

RFP Section	Exception
Attachment D, IT Terms, Sec 1, 1.8	The following section is hereby deleted in its entirety and is replaced by the following: **Personal Data** means any 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) any personally-identifiable information subject to protection under federal, state or local law, rule, regulation or ordinance.
Attachment D, IT Terms, Sec 1, 1.9	The following section is hereby deleted in its entirety and is replaced by the following: **"Security Incident** means the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.
Attachment D, IT Terms, Section 9, Source Code Escrow	**This section is hereby deleted in its entirety.**
Attachment D, IT Terms, Section 11, Ownership Rights	**Section 11 "Ownership Rights" is hereby deleted in its entirety and is replaced with the following:** **"Intellectual Property** Subject to the express rights and licenses granted by Juniper under this Agreement, Customer acknowledges and agrees that: (i) any and all intellectual property rights in or to the hardware, software, services, and/or cloud services are the sole and exclusive property of Juniper or its licensors; (ii) Customer shall not acquire any ownership

RFP Section	Exception
	interest in any such intellectual property rights under this Agreement; and (iii) if Customer acquires any intellectual property right in or relating to any product or services sold or licensed under this Agreement (including any right in any derivative works or patent improvements relating thereto), by operation of law, or otherwise, such rights are deemed and are hereby irrevocably assigned to Juniper, without further action by either party."
Attachment D, IT Terms, Appx 1. Section A, A.1, Customer Data	**The following section is hereby deleted in its entirety and is replaced with the following:** "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 and contractors with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein)."
Attachment D, IT Terms, Appx 1. Section B, B.4	**The following section is hereby deleted in its entirety and is replaced with the following:** "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. Notwithstanding the foregoing, Customer acknowledges and agrees that Customer Data may be processed by Supplier at its locations globally for purposes of the provision of support services."
Attachment D, IT Terms, Appx 1. Section B, B.5	**The following** section is hereby deleted in its entirety and is replaced with the following**:** **"**Upon the Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Supplier shall make available to the Customer information reasonably necessary to substantiate Supplier's compliance with the terms of Attachment D. If no such information is available at the time of the Customer's request, Supplier will provide Customer with signed, written

RFP Section	Exception
	attestation stating the same. Supplier will allow and cooperate in audits as set forth below. Customer shall have the right to carry out on-site audits (no more than once per year), during regular business hours without disrupting the Supplier's business operations and in accordance with Supplier's security policies. Any third party engaged by the Customer to conduct an audit must be pre-approved by Supplier (such approval not to be unreasonably withheld) and sign Juniper Networks' confidentiality agreement."
Attachment D, IT terms, Appendix 1, D.4	**The following section is hereby deleted in its entirety and is replaced with the following:** "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 forty-eight (48) 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.
Attachment D, IT Terms, Appendix 1, E.2	**The following section is hereby deleted in its entirety and is replaced with the following:** "E.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." The foregoing costs shall be subject to the limitations on liability set forth in the Contract."

RFP Section	Exception
Attachment D, IT Terms, Appendix 1, E.3	**This section is hereby deleted in its entirety and is replaced by the following:** "E.3 Subject to the limitations of liability set forth in the Contract 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.
Attachment D, IT Terms, Appendix 1, F	The following is added to Attachment D, Appx. 1, F: Notwithstanding the foregoing, where the notice concerns a Security Incident impacting multiple of Supplier's customers, notification shall be provided to the email address(es) of record registered within Supplier's customer portal.
Attachment D, IT Terms, Appendix 1, Section G.	**This section is hereby deleted in its entirety and replaced by the following:** "Supplier represents 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

Signature: Felicia A. Clark

Email: felicia.clark@omes.ok.gov

RFP Section	Exception
	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."
Attachment D, IT Terms, Appendix 1, Section I, I.1	**This section is hereby deleted in its entirety and is replaced by the following:** "1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data except for automatic deletions of data stored temporarily in Supplier's Cloud Services."
Attachment D, IT Terms, Appendix 1, Section I, I.2 (d)	**The following subsection is inserted into Section I.2 as item (d):** "Customer acknowledges that Supplier does not provide data storage solutions. In the event of a termination or expiration of the Contract, Customer shall fulfill its obligations to delete, destroy or return all copies of the software and any Confidential Information as set forth in the Contract between the parties. If, upon the termination of the Contract, Customer reasonably believes that Supplier possesses Customer Data that is needed by Customer for commercial or business continuity purposes, then Customer shall make a written request for the return of such Customer Data and Supplier will use commercially reasonable efforts to return such Customer Data as agreed between the parties. "
Attachment D, IT Terms, Appendix 1, Section I, I.3	**This section is hereby deleted in its entirety and is replaced by the following:** **1.** "Subject to any automatic deletion cycles associated with Supplier's cloud services,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."

EXECUTION VERSION SW1006J Contract State of OK Juniper Networks2

Final Audit Report 2022-06-17

Created:	2022-06-16
By:	Sean Tolbert (Sean.Tolbert@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAc7AF5auv7Ccsti9mnB6ARJyiGW3fyYyO

"EXECUTION VERSION SW1006J Contract State of OK Juniper Networks2" History

Document created by Sean Tolbert (Sean.Tolbert@omes.ok.gov)
2022-06-16 - 6:14:25 PM GMT- IP address: 165.225.216.110

Document emailed to tbunting@juniper.net for signature
2022-06-16 - 6:15:44 PM GMT

Email viewed by tbunting@juniper.net
2022-06-16 - 8:50:42 PM GMT- IP address: 163.116.146.116

Document e-signed by Tim Bunting (tbunting@juniper.net)
Signature Date: 2022-06-16 - 8:51:21 PM GMT - Time Source: server- IP address: 163.116.146.116

Document emailed to Felicia Clark (felicia.clark@omes.ok.gov) for signature
2022-06-16 - 8:51:23 PM GMT

Email viewed by Felicia Clark (felicia.clark@omes.ok.gov)
2022-06-17 - 1:27:18 PM GMT- IP address: 86.106.177.121

Document e-signed by Felicia Clark (felicia.clark@omes.ok.gov)
Signature Date: 2022-06-17 - 1:30:21 PM GMT - Time Source: server- IP address: 165.225.216.102

Document emailed to Jerry Moore (jerry.moore@omes.ok.gov) for signature
2022-06-17 - 1:30:23 PM GMT

Document e-signed by Jerry Moore (jerry.moore@omes.ok.gov)
Signature Date: 2022-06-17 - 2:25:59 PM GMT - Time Source: server- IP address: 165.225.216.90

Agreement completed.
2022-06-17 - 2:25:59 PM GMT