



State of Oklahoma

Office of Management and Enterprise Services

**ADDENDUM 1 TO THE
STATE OF OKLAHOMA STATEWIDE CONTRACT NO. 1111
WITH OKLAHOMA INTERACTIVE, LLC**

This Addendum 1 (“Addendum”) is an Amendment to the Contract awarded to Oklahoma Interactive, LLC in connection with Statewide Contract No. 1111 (“SW1111” or the “Contract”) and is effective April 23, 2019.

Recitals

Whereas, the State issued a Solicitation No. 0900000358 (“Solicitation”) for proposals to provide Point-of-Sale (POS) Credit Card Transaction Processing Systems, as more particularly described in the Solicitation;

Whereas, Oklahoma Interactive, LLC submitted a proposal which contained exceptions and additions to the Solicitation terms; and

Whereas, the State and Oklahoma Interactive, LLC have negotiated the final terms under which Oklahoma Interactive, LLC will perform the Services under the Contract.

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. Addendum Purpose.

This Addendum memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Oklahoma Interactive, LLC as of even date with execution of this Addendum. The parties agree that Supplier has not yet begun performance of work contemplated by the Solicitation.

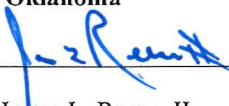
2. Negotiated Documents of the Contract.

2.1. The parties have negotiated certain terms of the Contract as follows:

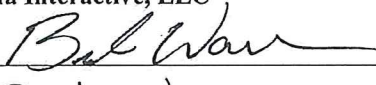
- i. certain exceptions and additions to the Solicitation as contained in Attachment A to this Addendum titled Negotiated Exceptions and Additional Terms to the Solicitation;

- ii. the State of Oklahoma's Hosting terms as contained in Attachment B to this Addendum titled Hosting Agreement; and
 - iii. the parties agree to utilize Section 3(C.8.) of Oklahoma Interactive, LLC's response as the terms for the service level agreement.
- 2.2. Any exceptions or additional terms submitted by Oklahoma Interactive, LLC that are not in Attachment A, are hereby denied.
- 2.3. The parties shall in good faith negotiate a statement of work to further define the scope of any State Entity or Interlocal Entity acquisition specific engagement.

State of Oklahoma

By: 
Name: James L. Reese, II
Title: Chief Information Officer
Date: 4/24/2019

Oklahoma Interactive, LLC

By: 
Name: Bret Warren
Title: General Manager
Date: 4/23/2019



State of Oklahoma

Office of Management and Enterprise Services

**ATTACHMENT A TO ADDENDUM 1 TO THE
STATE OF OKLAHOMA STATEWIDE CONTRACT NO. 1111
WITH OKLAHOMA INTERACTIVE, LLC**

Negotiated Exceptions and Additional Terms to the Solicitation

The Solicitation is hereby amended to include the terms as set forth below and supersedes all prior terms and Exceptions submitted by **Oklahoma Interactive** or discussed by the parties.

RFP Section	Exception
A. General Provisions, A.5.2. Legal Contract	<p>Section A, General Provisions, A.5.2. is hereby deleted in its entirety and replaced with the following:</p> <p>The Contract Documents resulting from this Solicitation shall have the following order of precedence: any Addendum or Amendment (including any attachments or exhibits thereto); this Solicitation (including any amendments thereto); and the successful Bid as amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law; any statement of work, work order, or other similar ordering document as applicable; any purchase order or other appropriate encumbrance document; and other mutually agreed Contract Documents.</p>
A. General Provisions, A.13. Delivery, Inspection and Acceptance	<p>Section A. General Provisions, A.13. is hereby modified to add the following provision as A.13.3:</p> <p>For Services provided under this Contract, the State shall review and accept any deliverables and the implementation of the system within 30 days of delivery of the same if the State makes a good faith determination that the deliverable materially meets the functional specifications called for in this Contract or the applicable SOW. If the deliverable does not meet the acceptance standard the State shall provide prompt written notice of why the deliverable failed acceptance and the Supplier shall have 30 days to correct the deficiency and resubmit the deliverable for acceptance.</p>
A. General Provisions, A.15.1. Audit and Records Clause	<p>Section A. General Provisions, A.15.1. is hereby deleted in its entirety and replaced with the following:</p> <p>As used in this clause, "records" includes books, documents, 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</p>

RFP Section	Exception
	<p>any other form. In accepting any contract with the State, the Supplier agrees any pertinent state or federal agency shall have the right to examine and audit all records relevant to the execution and performance of this Contract upon 15 days' advance written notice and no more than 1 time per calendar year.</p>
<p>A. General Provisions, A.18.1. Termination for Cause</p>	<p>Section A. General Provisions, A.18.1. is hereby deleted in its entirety and replaced with the following:</p> <p>Supplier may terminate the Contract in whole or may terminate a SOW or SOWs in the event (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. Material breach by a Customer shall 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 in the event (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. Similarly, a Customer may terminate its obligations, in whole, 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.</p>
<p>A. General Provisions, A.18.2. Termination for Cause</p>	<p>Section A. General Provisions, A.18.2. is hereby deleted in its entirety and replaced with the following:</p> <p>The State may terminate the Contract, in whole, 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 a product or service to the Customer or if (i) Supplier's material breach is reasonable determined to be a material impediment to the function of the State and materially detrimental to the State; (ii) Supplier material breach is reasonable determined 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 .For the avoidance of doubt, such a termination pursuant to (iii) of this Section shall not be considered a termination for Contractor's breach.</p> <p>The Customer may terminate a SOW 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 to be a material</p>

RFP Section	Exception
	impediment to the function of the Customer and materially detrimental to the Customer or (ii) when conditions preclude the thirty (30) day notice.
A. General Provisions, A.19.2 Termination for Convenience	<p>Section A. General Provisions, A.19.2. is hereby deleted in its entirety and replaced with the following:</p> <p>The State may terminate this Contract, in whole, for convenience if the State Chief Information Officer determines that termination is in the State's best interest. The State shall terminate this Contract by delivering to the Supplier a notice of termination for convenience specifying the terms and effective date of termination. The Contract termination date shall be a minimum of sixty (60) days from the date the notice of termination is issued by the State. Similarly, an Interlocal Entity may terminate its obligations to Supplier upon a determination by the proper authority for such Interlocal Entity that termination is in the Interlocal Entity's best interest and notice of termination by such Interlocal Entity shall be provided in accordance with the foregoing requirements set forth in this subsection.</p>
A. General Provisions, A.20. Insurance	<p>Section A. General Provisions, A.20. is hereby deleted in its entirety and replaced with the following:</p> <p>The Supplier shall maintain and promptly provide proof to the State of the following insurance coverage, and any renewals, as long as the Supplier has any obligation under a Contract Document:</p> <ul style="list-style-type: none"> a) Worker's Compensation and Employer's Liability Insurance in accordance with applicable law; b) Commercial General Liability Insurance on a per occurrence basis with limits of liability \$1,000,000 per occurrence and aggregate, combined single limit Personal Injury, Bodily Injury and Property Damage; c) Commercial Automobile Liability Insurance with limits of liability of \$1,000,000 per accident combined single limit including bodily injury and property damage and with coverage, if applicable, for all owned vehicles (if any), all non-owned vehicles, and all hired vehicles; d) Professional Errors and Omissions Insurance which shall include Consultant's Computer Errors and Omissions Coverage with limits \$1,000,000 per claim and in the aggregate.
A. General Provisions, A.28.1. Confidentiality	<p>Section A. General Provisions, A.28.1. is hereby replaced in its entirety with the following provision:</p> <p>The Supplier shall use commercially reasonable efforts to maintain strict security of all State 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 or records only as needed by Supplier for performance of its obligations hereunder. 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. If Supplier utilizes a permitted subcontractor, Supplier shall</p>

RFP Section	Exception
	<p>obtain specific written assurance, and provide a copy to the State, that the subcontractor shall maintain this same level of security of all data and records entrusted to or accessed by the subcontractor and agree to the same obligations as Supplier, to the extent applicable. Such written assurance may be set forth in the required subcontractor agreement referenced herein.</p>
<p>A. General Provisions, A.28.2. Confidentiality</p>	<p>Section A. General Provisions, A. 28.2. is hereby replaced in its entirety with the following provision:</p> <p>No State data or records shall be provided or the contents thereof disclosed to a third party unless specifically authorized to do so in writing by the State CIO or in compliance with a valid court order. The Supplier shall immediately forward to the State and the State CIO 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 commercially reasonable efforts to protect the security and confidentiality of such data or records in response to a third party request.</p>
<p>A. General Provisions, A.28. Confidentiality</p>	<p>Section A. General Provisions, A.28. is modified to add the following provision as A.28.3.:</p> <p>Supplier Confidential Information means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed in good faith by the State Purchasing Director or Customer, as applicable, that such information is legally able to be protected under applicable law. Supplier Confidential Information does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act. In addition, "Confidential Information" of Supplier shall include, but not be limited to, the following:</p> <ul style="list-style-type: none"> • All books, records, documents, and electronic files that pertain to Supplier's business or operation or to that of any of its affiliates which are clearly marked as confidential or that Supplier otherwise identifies as Confidential Information and all system source code, unless the same are disclosed publicly by Supplier or its corporate parent, affiliate or subsidiary. Such materials are the property of Supplier or its affiliate and are not system records; • Applications (including Supplier's intellectual property) and related documentation furnished or developed in connection with the Services, and the trade secrets and business methods of Supplier in operating the system provided. • Customer may be provided access to Supplier Confidential Information. If Customer is a state agency, Customer is subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent required under the Open Records Act and in accordance with this section. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use

RFP Section	Exception
	<p>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 by the Customer 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 Customer is required by law or regulation to disclose 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. For avoidance of doubt, if a request is made for disclosure of Supplier's Intellectual Property, Supplier shall be notified of the request and the State will reasonably assist the Supplier in obtaining a court order or other protection against disclosure provided the State has no obligation to expend funds, allocate resources as part of its cooperation or provide cooperation that interferes with any law enforcement investigation which is the basis for the request.</p> <p>The parties agree, to the extent such information falls within an exemption under the Open Records Act to (a) treat and keep as confidential all Confidential Information disclosed by the other party; (b) advise each employee to whom any Confidential Information is to be made available of the confidential nature of such Confidential Information and of each party's confidentiality obligations; (c) promptly return to the disclosing party (or its designees), upon the disclosing party's request, all Confidential Information and all copies thereof and, unless specifically granted a right to use under the terms of the Contract, to delete from electronic memory such Confidential Information.</p>
A. General Provisions, A.31.3 Patents and Copyrights	<p>Section A. General Provisions, A.31.3. second sentence is hereby modified as follows:</p> <p>If the Supplier determines that none of these alternatives is reasonably available, the State shall return such portion of the products at issuer to the Supplier, upon written request, in exchange for a refund of the price paid for such returned physical goods (such as the swipe devices purchased by the State or a Customer) as well as a refund, if applicable, of other physical goods purchased under this Contract which are rendered materially unusable as intended due to the removal of the portion of products at issue. For the avoidance of doubt, no such refund(s) shall include any payment processing fees paid by the State, a Customer, or end users.</p>

RFP Section	Exception
A. General Provisions, A.37. Limitation of Liability	<p>Section A. General Provisions, A.37. is hereby deleted in its entirety and replaced with the following:</p> <p>NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN, UNLESS OTHERWISE PROVIDED IN APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE FOR CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR INDIRECT DAMAGES, LOST PROFITS OR OTHER BUSINESS INTERRUPTION DAMAGES, IN TORT OR CONTRACT, EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN, EXCEPT FOR INTELLECTUAL PROPERTY INFRINGEMENT, SUPPLIER'S FRAUD OR WILLFUL MISCONDUCT AND EXCEPT FOR THE OBLIGATION TO REMIT FUNDS COLLECTED ON BEHALF OF THE STATE, IN NO EVENT SHALL SUPPLIER BE LIABLE FOR LOSSES, DAMAGES OR INDEMNITIES ARISING OUT OF OR RELATED TO THIS CONTRACT EXCEED THE AMOUNT PAID OR TO BE PAID TO SUPPLIER FOR ITS SERVICES UNDER THE SPECIFIC ENGAGEMENT, STATEMENT OF WORK, OR OTHER SIMILAR CONTRACT DOCUMENT GIVING RISE TO THE CLAIM. THE FOREGOING PROVISIONS OF THE SECTION SHALL NOT APPLY TO OR LIMIT DAMAGES, EXPENSES, COSTS, ACTIONS, CLAIMS AND LIABILITIES ARISING FROM OR RELATED TO (1) PROPERTY DAMAGE, BODILY INJURY OR DEATH CAUSED BY SUPPLIER'S NEGLIGENCE OR WILLFUL MISCONDUCT; (2) THE INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS CONTRACT; (3) SUPPLIER'S CONFIDENTIALITY OBLIGATIONS SET FORTH IN THIS CONTRACT; (4) DATA SECURITY AND BREACH NOTIFICATION OBLIGATIONS SET FORTH IN THE CONTRACT; (5) THE BAD FAITH, GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT OF SUPPLIER OR ITS EMPLOYEES AGENTS AND SUBCONTRACTORS; OR (6) OTHER ACTS FOR WHICH APPLICABLE LAW DOES NOT ALLOW EXEMPTION FROM LIABILITY (THE PRECEDING EXEMPTIONS 1-6 ARE REFERRED TO HEREIN AS "EXEMPT CLAIMS").</p> <p>FOR EXEMPT CLAIMS, THE CONTRACTOR'S AGGREGATE LIABILITY UNDER THIS CONTRACT SHALL BE LIMITED TO \$5,000,000.</p>
A. General Provisions, A.38.2. Media Ownership (Disk Drive and/or Memory Chip Ownership)	<p>Section A. General Provisions, A.38. is hereby modified to add the following provision as A.38.3.:</p> <p>Notwithstanding anything to the contrary herein, the parties acknowledge that if the system is hosted with a cloud-service provider or on a multi-tenant</p>

RFP Section	Exception
	basis, the requirements in this Article 38 shall apply to such media devices and components.
A. General Provisions, A.44. Emerging Technologies	<p>Section A. General Provisions, A.44 is hereby deleted in its entirety and replaced with the following provision:</p> <p>The State of Oklahoma reserves the right to request a modification of the terms of this Contract at any time to allow for technologies not identified in this Contract. If there are repeated requests for an “emerging technology” and the State feels it is warranted to add such technologies, the State may request to add such technology. Upon any such request, the parties agree to negotiate in good faith to mutually agreeable Amendment to this Contract.</p>
A. General Provisions, A.45.1. Ownership Rights	<p>Section A. General Provisions, A.45.1 is hereby deleted in its entirety and replaced with the following:</p> <p>Should Supplier develop any software under this Contract for the sole and exclusive use of the State, then, pursuant to the terms of the applicable SOW, the State shall enjoy, including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on the Utilities, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Utilities embodied in any software developed under this Contract for the sole and exclusive use of the State, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy modify, display, perform, transmit and prepare derivative works of Utilities embodied or delivered to the State in conjunction with the products.</p>
A. General Provisions, A.45.1. Ownership Rights	<p>Section A. General Provisions, A.45.1 is hereby added:</p> <p>All State trademarks, trade names, logos, and other State identifiers, Internet uniform resource locators, Internet addresses and e-mail addresses obtained or developed pursuant to this contract shall be the property of the State. All content and all property, data and information furnished by or on behalf of the State to Supplier under this contract shall be and remain the sole property of the State.</p>
A. General Provisions, A.45.2. Ownership Rights	<p>Section A. General Provisions, A.45.2(a) is hereby added:</p> <p>Notwithstanding anything herein to the contrary, each party shall retain all of its pre-existing ownership rights, title and interest in its pre-existing intellectual property, subject to any licenses explicitly granted herein. For the avoidance of doubt, any enhancements to Supplier’s existing software or</p>

RFP Section	Exception
	<p>other intellectual property, and any software or intellectual property created during the term of this Contract that is not for the sole use of the State, shall be owned by Supplier and shall not be a "Work Made for Hire." The State shall receive the same license to any such software or intellectual property as provided for in A.45.3(a).</p>
<p>A. General Provisions, A.45.3. Ownership Rights</p>	<p>Section A. General Provisions, A.45.3 is hereby deleted in its entirety and replaced with the following:</p> <p>In the event that it should be determined that any portion of the software developed under this Contract for the sole and exclusive use of the State or related supporting documentation does not qualify as "Work Made for Hire", Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Utilities embodied in or delivered to the State in conjunction with such software that was intended to be a "Work Made for Hire".</p>
<p>A. General Provisions, A.45.3. Ownership Rights</p>	<p>Section A. General Provisions, A.45.3(a) is hereby added:</p> <p>For the software currently contemplated to be provided as part of the Services under the Contract, Supplier grants to the State a license to such software and services provided hereunder for the term of this contract. During the term of this contract, Supplier will provide access to the functionality of the software and services contracted for herein for the purpose set forth herein or in any SOW or change order (the "Permitted Uses"). In the interest of clarity, Permitted Uses excludes any sale, licensing, or other transfer for commercial purposes, including transfer or sublicense to any other third-party, including any other state, federal agency or unit, or local agency or unit of government, except as otherwise provided herein. The State's license and access to the software and services shall terminate upon the termination or expiration of this Contract; provided, however, to the extent a SOW survives the expiration or termination of this Contract, the State's license shall continue for the term of that SOW. The State does not have any rights to have or make copies or archival copies of any software (or source code) used in the services during the term of this Contract or following its termination or expiration, unless otherwise stated herein. For the avoidance of doubt, 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.</p>
<p>A. General Provisions, A.45.4. Ownership Rights</p>	<p>Section A. General Provisions, A.45.4 first sentence is hereby replaced with the following:</p> <p>Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized under this Contract for the sole and exclusive use of the State, ("Works for Hire"). Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall</p>

RFP Section	Exception
	bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.
A. General Provisions, A.45.4. Ownership Rights	<p>Section A. General Provisions, A.45.4 is hereby modified to add the following provision as A.45.4.(a):</p> <p>In the event any credit card swipe devices are utilized in the services, then after the Contract has expired, and if all available term extensions were exercised, the ownership of such swipe devices shall be transferred to the State (for the sole benefit of the State) by Supplier, to the extent permissible under the applicable third-party license terms. Supplier makes no warranties with respect to the swipe devices and other materials after termination or expiration of the Contract, and the only warranties the State receives at that time are the transferable manufacturer warranties, if any.</p>
A. General Provisions, A.45.6. Ownership Rights	<p>Section A. General Provisions, A.45.6 is hereby deleted and replaced with:</p> <p>For the avoidance of doubt, the Services currently contemplated under this Contract do not include custom development work or other development work for which the State will receive a perpetual license or ownership, except as outlined herein. In the event the parties amend this Contract to include customer development work or works made for hire, then the parties agree to negotiate in good faith additional license and/or ownership terms as part of that amendment.</p>
A. General Provisions, A.45.7. Ownership Rights	Section A. General Provisions, A.45.7 is hereby deleted in its entirety.
A. General Provisions, A.46. Source Code Escrow	<p>Section A. General Provisions, A.46. is hereby modified to add the following provision:</p> <p>Notwithstanding anything to the contrary herein, no escrow is currently required of the SaaS solution being provided by the Supplier. If the Services are modified in such a way that Supplier that Title 62 O.S. § 34.31 becomes applicable, then Supplier and the State will negotiate in good faith to add escrow related terms and conditions to this Contract to cover any such applications. Any such escrow terms and conditions will be in accordance with applicable statutes.</p>
A. General Provisions, A.49. Publicity	<p>Section A. General Provisions, A.49 is hereby modified to add the following sentence to the end of the provision:</p> <p>Nothing herein shall require approval of or shall prevent Supplier or its parent company from making any public disclosure or report that is prudent or required under applicable laws or regulations, including but not limited to securities laws and the requirements of Nasdaq.</p>
B. Special Provisions, B.3. Warrants	<p>Section B. General Provisions, B.3. is hereby deleted in its entirety and replaced with the following provision:</p> <p>Supplier warrants and represents that products or deliverables specified and furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, conform to the functional specifications and requirements for a warranty period of a minimum of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer (for third-party software and hardware). Defects in products or deliverables specified and furnished by or through the Supplier</p>

RFP Section	Exception
	<p>that do not meet the standard in the preceding sentence shall be repaired or replaced by Supplier at no cost or expense to the State if such defect occurs during the warranty period.</p>
<p>B. Special Provisions, B.13. Force Majeure</p>	<p>Section B. General Provisions, B.13 is hereby added:</p> <p>Either party shall be temporarily excused from performance to the extent delayed or unable to perform as a result of causes beyond its reasonable control including fire or other similar casualty, act of God, terrorist activities, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority, or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all commercially reasonable steps within the party's control to ensure continued performance and to shorten duration of the event ("Force Majeure Event"). In the event that a party's performance of its obligations is materially hindered as a result of a Force Majeure Event, such party shall (a) promptly provide written notice to the other party of its best reasonable assessment of the nature and duration of the Force Majeure Event and the 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 result full performance as soon as reasonably practicable. Subject to the conditions set forth above, such non-performance shall not be deemed a default. However, if a Force Majeure Event extends beyond 30 days, the affected SOWs may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of the Customer. Supplier shall not invoice state for any period Supplier cannot perform due to a Force Majeure event and will refund any fees prepaid but not used during a Force Majeure event.</p> <p>Notwithstanding the foregoing or any other provision in the Contract, (1) in no event will any of the following be considered a force majeure event: (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 (2) no Force Majeure Event modifies or excuses Supplier's obligations related to confidentiality, indemnification or data security and breach notifications set forth herein.</p>

**ATTACHMENT B TO ADDENDUM 1 TO THE
STATE OF OKLAHOMA STATEWIDE CONTRACT NO. 1111
WITH OKLAHOMA INTERACTIVE, LLC**

HOSTING AGREEMENT

This Hosting Agreement (“Hosting Agreement”) is a Contract Document in connection with the Statewide Contract No. 1111 (“SW1111” or the “Contract”) and entered into between Oklahoma Interactive, LLC (“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 Non-Public Data or Personal 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) an individual’s name in combination with any of the following: 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 (as defined in HIPAA) that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended.
- e. “Security Incident” shall mean the attempted unauthorized access, use, disclosure, modification, or destruction that is confirmed to be targeted at Customer Data. Security Incident shall include the successful unauthorized access, use, disclosure, modification, or destruction of Customer Data that does not constitute Non-Public Data or Personal Data.

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 contact the OMES Service Desk via email as set forth in Section VII 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. Except as otherwise prohibited by law, Vendor agrees to provide its completed responses to the Customer for Customer review, revision and approval no later than two business days prior to the date such response is due.
- 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 upon its knowledge 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 commercially reasonable 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 shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Vendor is responsible for encryption of Personal Data on its systems and that is transmitted by its systems.
- c. Each party represents and warrants to the other party that its hosting equipment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. The parties will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Each party 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 the other party, the party where the virus originated will promptly notify the other party of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means such party has used 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: Vendor shall inform Customer of any Security Incident.

- 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 there is a Security Incident, the parties will coordinate prior to making any such communication.
- b. Vendor shall report a Security Incident that does not involve successful unauthorized access, use, disclosure, modification or destruction of Customer Data 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.
- d. If Vendor has reasonable belief or actual knowledge of a Security Incident that involved successful unauthorized access, use, disclosure, modification, or destruction of Customer Data, then Vendor shall (1) promptly notify the appropriate Customer identified contact set forth herein within 2 business days or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address such Security Incident in a timely manner.

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 business hours, unless shorter time is required by applicable law, after 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. If there is a Data Breach, the parties will coordinate prior to making any public communication or communication with parties who are not part of this Contract.
- b. Unless otherwise stipulated, if a Data Breach is a direct result of Vendor's breach of its obligation to encrypt or redact Personal Data or otherwise prevent a Data Breach of unencrypted or unredacted Personal Data stored in its hosted environment, 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 or redact Personal Data or otherwise prevent a Data Breach of unencrypted or unredacted Personal Data stored in its hosted environment, then Vendor shall indemnify and hold harmless the Customer against all penalties assessed to indemnified parties by governmental authorities in connection with the Data Breach.
- d. Costs associated with Vendor's Data Breach Responsibilities set forth in Sections VI.(b) or (c) shall be reduced to reflect any apportionment of fault attributed to the Customer's negligence, willful misconduct or breach of contract that caused 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

For immediate notice which does not constitute written notice:

OMES Service Desk

405-521-2444

Servicedesk@omes.ok.gov

Attn: Chief Information Security Officer

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

- a. Vendor will use commercially reasonable methods to 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.
- b. 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.
- c. The parties shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through 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. 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.

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.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]